

09/807824

PCT/JP00/05543

18.08.00

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 04 SEP 2000

WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

1999年12月21日

エジュ

出願番号
Application Number:

平成11年特許願第363266号

出願人
Applicant(s):

ソニー株式会社

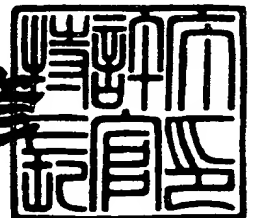
PRIORITY
DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 6月29日

特許庁長官
Commissioner,
Patent Office

近藤 隆彦



出証番号 出証特2000-3050085

【書類名】 特許願
【整理番号】 9900664607
【提出日】 平成11年12月21日
【あて先】 特許庁長官殿
【国際特許分類】 G11B 7/00
【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 浅野 智之

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 大澤 義知

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100067736

【弁理士】

【氏名又は名称】 小池 晃

【選任した代理人】

【識別番号】 100086335

【弁理士】

【氏名又は名称】 田村 榮一

【選任した代理人】

【識別番号】 100096677

【弁理士】

【氏名又は名称】 伊賀 誠司

【先の出願に基づく優先権主張】

【出願番号】 平成11年特許願第234371号

【出願日】 平成11年 8月20日

【手数料の表示】

【予納台帳番号】 019530

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707387

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報記録／再生システム、情報記録／再生装置及び方法、情報記録媒体、記録媒体製造装置及び方法

【特許請求の範囲】

【請求項 1】 セキュリティモジュールを有する情報記録媒体と、上記セキュリティモジュールが管理する暗号鍵によって暗号化されたデータを上記情報記録媒体に記録、あるいは、上記セキュリティモジュールが管理する暗号鍵によって暗号化されたデータを上記情報記録媒体から再生する情報記録／再生装置とを備え、

情報記録時、又は情報再生時に上記情報記録／再生装置とセキュリティモジュールとが公開鍵暗号技術を用いた相互認証プロトコルを実行することを特徴とする情報記録／再生システム。

【請求項 2】 上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、互いに、他方の識別情報がリボケーションリストに掲載されていないことを確認することを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 3】 上記セキュリティモジュールと上記情報記録／再生装置の何れか一方若しくは両方がリボケーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 4】 上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、互いに、自分が所有するリボケーションリストのバージョンナンバーを教え合い、新しいリボケーションリストを持つものがそれを他方に送り、古いリボケーションリストを持つものは送られた新しいリボケーションリストを用いて自分のリボケーションリストを置き換えることを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 5】 上記記録／再生装置とセキュリティモジュールの両者は、共に上記新しいリボケーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項 4 記載の情報記録／再生システム。

【請求項 6】 上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、互いに、他方の識別情報がレジストレーションリストに登録されていることを確認することを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 7】 上記セキュリティモジュールと上記情報記録／再生装置の何れか一方若しくは両方がレジストレーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 8】 上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、互いに、自分が所有するレジストレーションリストのバージョンナンバーを教え合い、~~新しいレジストレーションリストを持つものが~~それを他方に送り、古いレジストレーションリストを持つものは送られた新しいレジストレーションリストを用いて自分のレジストレーションリストを置き換えることを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 9】 上記記録／再生装置とセキュリティモジュールの両者は、共に上記新しいレジストレーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項 8 記載の情報記録／再生システム。

【請求項 10】 上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、互いに、他方の識別情報がリボケーションリストに掲載されていないこと、及び／又は、レジストレーションリストに登録されていることを確認することを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 11】 上記セキュリティモジュールと上記情報記録／再生装置の何れか一方若しくは両方がリボケーションリスト及びレジストレーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 12】 上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、互いに、自分が所有するリボケーションリスト及びレジストレーションリストのバージョンナンバーを教え合い、新しいリボケーションリスト及びレジストレーションリストを持つものがそれを他方に送り、古い

リボケーションリスト及びレジストレーションリストを持つものは送られた新しいリボケーションリスト及びレジストレーションリストを用いて自分のリボケーションリスト及びレジストレーションリストを置き換えることを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 1 3】 上記記録／再生装置とセキュリティモジュールの両者は、共に上記新しいボケーションリスト及び／又はレジストレーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項 1 2 記載の情報記録／再生システム。

【請求項 1 4】 上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、リボケーションリストとレジストレーションリストのうち何れか一方を選択的に使用することを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 1 5】 データの記録時又は再生時に、上記情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを暗号化する暗号鍵を一方が暗号化して他方に送ることを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 1 6】 データの記録時又は再生時に、上記情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを一方が暗号化して他方に送ることを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 1 7】 データを格納する情報記録媒体への書き込み、読み出しのアクセスは、上記セキュリティモジュールを介して行われることを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 1 8】 データの記録時に、上記情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いて上記情報記録／再生装置がデータを暗号化してセキュリティモジュールに送り、上記セキュリティモジュールは、共有された鍵を用いてこれを復号して平文データを得た後に、暗号鍵を用いてデータを暗号化して情報記録媒体に格納することを特徴とする請求項 1 7 記載の情報記録／再生システム。

【請求項 1 9】 データの再生時に、上記セキュリティモジュールが暗号化されて情報記録媒体に格納されているデータを読み出し、暗号鍵を用いてこれを復号して平文データを得た後、上記情報記録／再生装置とセキュリティモジュールが鍵共有プロトコルを実行した結果共有された鍵を用いてデータを上記セキュリティモジュールが暗号化して情報記録／再生装置に送ることを特徴とする請求項 1 7 記載の情報記録／再生システム。

【請求項 2 0】 データの記録時及び再生時に、情報記録／再生装置との間で公開鍵暗号を用いた相互認証プロトコルを実行するセキュリティモジュールを有することを特徴とする情報記録媒体。

【請求項 2 1】 上記セキュリティモジュールは、上記相互認証プロトコルを実行するときに、~~情報記録／再生装置の識別情報がリボケーションリストに掲載~~されていないことを確認することを特徴とする請求項 2 0 記載の情報記録媒体。

【請求項 2 2】 上記セキュリティモジュールは、自分と上記情報記録／再生装置の何れか一方若しくは両方がリボケーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴とする請求項 2 0 記載の情報記録媒体。

【請求項 2 3】 上記セキュリティモジュールは、上記相互認証プロトコルを実行するときに、自分が持つリボケーションリストのバージョンナンバーを情報記録／再生装置に送り、これと上記情報記録／再生装置が送ったリボケーションリストのバージョンナンバーを受信して比較し、自分のものの方が新しい場合にはリボケーションリストを相手に送り、相手のものの方が新しい場合には、相手から送られたリボケーションリストを現在自分が持っているものと置き換える処理を行うことを特徴とする請求項 2 0 記載の情報記録媒体。

【請求項 2 4】 上記セキュリティモジュールは、自分と上記情報記録／再生装置が持つリボケーションリストのうち、新しいリボケーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項 2 3 記載の情報記録媒体。

【請求項 2 5】 上記セキュリティモジュールは、上記相互認証プロトコルを実行するときに、情報記録／再生装置の識別情報がレジストレーションリストに

登録されていることを確認することを特徴とする請求項 2 0 記載の情報記録媒体

【請求項 2 6】 上記セキュリティモジュールは、自分と上記情報記録／再生装置の何れか一方若しくは両方がレジストレーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴とする請求項 2 0 記載の情報記録媒体。

【請求項 2 7】 上記セキュリティモジュールは、上記相互認証プロトコルを実行するときに、自分が持つレジストレーションリストのバージョンナンバーを情報記録／再生装置に送り、これと上記情報記録／再生装置が送ったレジストレーションリストのバージョンナンバーを受信して比較し、自分のものの方が新しい場合にはレジストレーションリストを相手に送り、相手のものの方が新しい場合には、相手から送られたレジストレーションリストを現在自分が持っているものと置き換える処理を行うことを特徴とする請求項 2 0 記載の情報記録媒体。

【請求項 2 8】 上記セキュリティモジュールは、自分と上記情報記録／再生装置が持つレジストレーションリストのうち、新しいレジストレーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項 2 7 記載の情報記録媒体。

【請求項 2 9】 上記セキュリティモジュールは、上記相互認証プロトコルを実行するときに、情報記録／再生装置の識別情報がリボケーションリストに掲載されていないこと、及び／又は、レジストレーションリストに登録されていることを確認することを特徴とする請求項 2 0 記載の情報記録媒体。

【請求項 3 0】 上記セキュリティモジュールは、自分と上記情報記録／再生装置の何れか一方若しくは両方がリボケーションリスト及びレジストレーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴とする請求項 2 0 記載の情報記録媒体。

【請求項 3 1】 上記セキュリティモジュールは、上記相互認証プロトコルを実行するときに、自分が持つリボケーションリスト及びレジストレーションリストのバージョンナンバーを情報記録／再生装置に送り、これと上記情報記録／再生装置が送ったリボケーションリスト及びレジストレーションリストのバージョ

ンナンバーを受信して比較し、自分のものの方が新しい場合にはリボケーションリスト及びレジストレーションリストを相手に送り、相手のものの方が新しい場合には、相手から送られたリボケーションリスト及びレジストレーションリストを現在自分が持っているものと置き換える処理を行うことを特徴とする請求項 20 記載の情報記録媒体。

【請求項 32】 上記セキュリティモジュールは、自分と上記情報記録／再生装置が持つリボケーションリスト及び／又はレジストレーションリストのうち、新しいリボケーションリスト及び／又はレジストレーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項 31 記載の情報記録媒体。

~~【請求項 33】 上記セキュリティモジュールは、上記相互認証プロトコルの~~
実行時に、リボケーションリストとレジストレーションリストのうち何れか一方を選択的に使用することを特徴とする請求項 20 記載の情報記録媒体。

【請求項 34】 上記セキュリティモジュールが管理する暗号鍵を用いて暗号化されたデータを格納することを特徴とする請求項 20 記載の情報記録媒体。

【請求項 35】 上記セキュリティモジュールは、データの記録時及び再生時に、情報記録／再生装置との間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて、データを暗号化する暗号鍵を情報記録／再生装置に送信あるいは情報記録／再生装置から受信することを特徴とする請求項 20 記載の情報記録媒体。

【請求項 36】 データの書き込み及び読み出しの処理が上記セキュリティモジュールを介して行われることを特徴とする請求項 20 記載の情報記録媒体。

【請求項 37】 上記セキュリティモジュールは、データの記録時に、情報記録／再生装置との間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて受信したデータを復号し、さらに別の鍵を用いてデータを暗号化することを特徴とする請求項 36 記載の情報記録媒体。

【請求項 38】 データの再生時に、記録媒体からデータを読み出して暗号鍵 1 を用いて復号した後、情報記録／再生装置との間で公開鍵暗号を用いた鍵共有プロトコルを実行し、共有した鍵を用いてデータを暗号化して情報記録／再生装

置に送信することを特徴とする請求項 3 6 記載の情報記録媒体。

【請求項 3 9】 データの記録時及び再生時に、情報記録媒体のセキュリティモジュールとの間で公開鍵暗号を用いた相互認証プロトコルを実行する制御手段を備えることを特徴とする情報記録／再生装置。

【請求項 4 0】 上記制御手段は、上記相互認証プロトコルを実行するときに、上記セキュリティモジュールの識別情報がリボケーションリストに掲載されていないことを確認することを特徴とする請求項 3 9 記載の情報記録／再生装置。

【請求項 4 1】 上記制御手段は、上記セキュリティモジュールを有する情報記録媒体と自分の何れか一方若しくは両方がリボケーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴とする請求項 3 9 記載の情報記録／再生装置。

【請求項 4 2】 上記制御手段は、上記相互認証プロトコルを実行するときに、自分が持つリボケーションリストのバージョンナンバーをセキュリティモジュールに送り、これと上記セキュリティモジュールが送ったリボケーションリストのバージョンナンバーを受信して比較し、自分のものの方が新しい場合にはリボケーションリストを相手に送り、相手のものの方が新しい場合には、相手から送られたリボケーションリストを現在自分が持っているものと置き換える処理を行うことを特徴とする請求項 3 9 記載の情報記録／再生装置。

【請求項 4 3】 上記制御手段は、自分と上記セキュリティモジュールの両者のもつリボケーションリストのうち、新しいリボケーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項 4 2 記載の情報記録／再生装置。

【請求項 4 4】 上記制御手段は、上記相互認証プロトコルを実行するときに、上記セキュリティモジュールの識別情報がレジストレーションリストに登録されていることを確認することを特徴とする請求項 3 9 記載の情報記録／再生装置。

【請求項 4 5】 上記制御手段は、上記セキュリティモジュールを有する情報記録媒体と自分の何れか一方若しくは両方がレジストレーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴と

する請求項 39 記載の情報記録／再生装置。

【請求項 46】 上記制御手段は、上記相互認証プロトコルを実行するときに、自分が持つレジストレーションリストのバージョンナンバーをセキュリティモジュールに送り、これと上記セキュリティモジュールが送ったレジストレーションリストのバージョンナンバーを受信して比較し、自分のものの方が新しい場合にはレジストレーションリストを相手に送り、相手のものの方が新しい場合には、相手から送られたレジストレーションリストを現在自分が持っているものと置き換える処理を行うことを特徴とする請求項 39 記載の情報記録／再生装置。

【請求項 47】 上記制御手段は、自分と上記セキュリティモジュールの両者のもつレジストレーションリストのうち、新しいレジストレーションリストを用いて、~~上記相互認証プロトコルを実行することを特徴とする請求項 46 記載の情報記録／再生装置。~~

【請求項 48】 上記制御手段は、上記相互認証プロトコルを実行するときに、上記セキュリティモジュールの識別情報がリボケーションリストに掲載されていないこと、及び／又は、レジストレーションリストに登録されていることを確認することを特徴とする請求項 39 記載の情報記録／再生装置。

【請求項 49】 上記制御手段は、上記セキュリティモジュールを有する情報記録媒体と自分の何れか一方若しくは両方がリボケーションリスト及びレジストレーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴とする請求項 39 記載の情報記録／再生装置。

【請求項 50】 上記制御手段は、上記相互認証プロトコルを実行するときに、自分が持つリボケーションリスト及びレジストレーションリストのバージョンナンバーをセキュリティモジュールに送り、これと上記セキュリティモジュールが送ったりボケーションリスト及びレジストレーションリストのバージョンナンバーを受信して比較し、自分のものの方が新しい場合にはリボケーションリスト及びレジストレーションリストを相手に送り、相手のものの方が新しい場合には、相手から送られたリボケーションリスト及びレジストレーションリストを現在自分が持っているものと置き換える処理を行うことを特徴とする請求項 39 記載の情報記録／再生装置。

【請求項 51】 上記制御手段は、自分と上記セキュリティモジュールの両者のもつリボケーションリスト及び／又はレジストレーションリストのうち、新しいリボケーションリスト及び／又はレジストレーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項 50 記載の情報記録／再生装置。

【請求項 52】 上記セキュリティモジュールは、上記相互認証プロトコルの実行時に、リボケーションリストとレジストレーションリストのうち何れか一方を選択的に使用することを特徴とする請求項 39 記載の情報記録／再生装置。

【請求項 53】 上記制御手段は、データの記録時及び再生時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて、データを暗号化する暗号鍵を上記セキュリティモジュールに送信あるいは上記セキュリティモジュールから受信することを特徴とする請求項 39 記載の情報記録／再生装置。

【請求項 54】 上記制御手段は、データの記録時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いてデータを暗号化して情報記録媒体に格納することを特徴とする請求項 39 記載の情報記録／再生装置。

【請求項 55】 上記制御手段は、データの記録時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いてデータを暗号化して上記セキュリティモジュールに送信することを特徴とする請求項 39 記載の情報記録／再生装置。

【請求項 56】 上記制御手段は、データの記録時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いてデータの暗号化に用いる暗号鍵を暗号化して上記セキュリティモジュールに送信し、又は共有した鍵を用いて暗号化された暗号鍵を上記セキュリティモジュールから受信し、上記暗号鍵を用いてデータを暗号化して上記セキュリティモジュールに送信することを特徴とする請求項 39 記載の情報記録／再生装置。

【請求項 5 7】 上記制御手段は、データの再生時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて、上記セキュリティモジュールから送られたデータを復号することを特徴とする請求項 3 9 記載の情報記録／再生装置。

【請求項 5 8】 上記制御手段は、データの再生時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて、データの暗号化に用いる暗号鍵を暗号化してセキュリティモジュールに送信し、又は共有した鍵を用いて暗号化された暗号鍵を上記セキュリティモジュールから受信し、上記暗号鍵を用いて上記セキュリティモジュールから送られたデータを復号することを特徴とする請求項 3 9 記載の情報記録／再生装置。

【請求項 5 9】 情報記録／再生装置により情報記録媒体にデータを記録、あるいは情報記録媒体からデータを再生する情報記録／再生方法において、

情報記録媒体が有するセキュリティモジュールと情報記録／再生装置が公開鍵暗号を用いた相互認証プロトコルを実行するステップを有することを特徴とする情報記録／再生方法。

【請求項 6 0】 上記相互認証プロトコルを実行するときに、情報記録／再生装置とセキュリティモジュールが、互いに、他方の識別情報がリボケーションリストに掲載されていないことを確認するステップを有することを特徴とする請求項 5 9 記載の情報記録／再生方法。

【請求項 6 1】 セキュリティモジュールと上記情報記録／再生装置の何れか一方若しくは両方がリボケーションリストを保持するか否かに応じた相互認証プロトコルを使用することを特徴とする請求項 5 9 記載の情報記録／再生方法。

【請求項 6 2】 上記相互認証プロトコルを実行するときに、情報記録／再生装置とセキュリティモジュールが、互いに、自分が所有するリボケーションリストのバージョンナンバーを教えるステップと、新しいリボケーションリストを持つものがそれを他方に送るステップと、古いリボケーションリストを持つものは送られた新しいリボケーションリストを用いて自分のリボケーションリストを置き換えるステップを有することを特徴とする請求項 5 9 記載の情報記録／再生方

法。

【請求項 6 3】 セキュリティモジュールと上記情報記録／再生装置が持つリボケーションリストのうち、新しいリボケーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項 6 2 記載の情報記録／再生方法。

【請求項 6 4】 上記相互認証プロトコルを実行するときに、情報記録／再生装置とセキュリティモジュールが、互いに、他方の識別情報がレジストレーションリストに掲載されていないことを確認するステップを有することを特徴とする請求項 5 9 記載の情報記録／再生方法。

【請求項 6 5】 セキュリティモジュールと上記情報記録／再生装置の何れか一方若しくは両方がレジストレーションリストを保持するか否かに応じた相互認証プロトコルを使用することを特徴とする請求項 5 9 記載の情報記録／再生方法。

【請求項 6 6】 上記相互認証プロトコルを実行するときに、情報記録／再生装置とセキュリティモジュールが、互いに、自分が所有するレジストレーションリストのバージョンナンバーを教えるステップと、新しいレジストレーションリストを持つものがそれを他方に送るステップと、古いレジストレーションリストを持つものは送られた新しいレジストレーションリストを用いて自分のレジストレーションリストを置き換えるステップを有することを特徴とする請求項 5 9 記載の情報記録／再生方法。

【請求項 6 7】 セキュリティモジュールと上記情報記録／再生装置が持つレジストレーションリストのうち、新しいレジストレーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項 6 6 記載の情報記録／再生方法。

【請求項 6 8】 上記相互認証プロトコルを実行するときに、情報記録／再生装置とセキュリティモジュールが、互いに、他方の識別情報がリボケーションリストに掲載されていないこと、及び／又は、レジストレーションリストに掲載されていないことを確認するステップを有することを特徴とする請求項 5 9 記載の情報記録／再生方法。

【請求項 6 9】 セキュリティモジュールと上記情報記録／再生装置の何れか一方若しくは両方がリボケーションリスト及びレジストレーションリストを保持するか否かに応じた相互認証プロトコルを使用することを特徴とする請求項 5 9 記載の情報記録／再生方法。

【請求項 7 0】 上記相互認証プロトコルを実行するときに、情報記録／再生装置とセキュリティモジュールが、互いに、自分が所有するリボケーションリスト及びレジストレーションリストのバージョンナンバーを教えるステップと、新しいリボケーションリスト及びレジストレーションリストを持つものがそれを他方に送るステップと、古いリボケーションリスト及びレジストレーションリストを持つものは送られた新しいリボケーションリスト及びレジストレーションリストを用いて自分のリボケーションリスト及びレジストレーションリストを置き換えるステップを有することを特徴とする請求項 5 9 記載の情報記録／再生方法。

【請求項 7 1】 セキュリティモジュールと上記情報記録／再生装置が持つリボケーションリスト及び／又はレジストレーションリストのうち、新しいリボケーションリスト及び／又はレジストレーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項 7 0 記載の情報記録／再生方法。

【請求項 7 2】 セキュリティモジュールと上記情報記録／再生装置は、上記相互認証プロトコルの実行時に、リボケーションリストとレジストレーションリストのうち何れか一方を選択的に使用することを特徴とする請求項 5 9 記載の情報記録／再生方法。

【請求項 7 3】 データの記録時又は再生時に、情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いた鍵共有プロトコルを実行するステップと、共有された鍵を用いてデータを暗号化する暗号鍵を一方が暗号化して他方に送るステップを有することを特徴とする請求項 5 9 記載の情報記録／再生方法。

【請求項 7 4】 データの記録時又は再生時に、情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いた鍵共有プロトコルを行うステップと、共有された鍵を用いてデータを一方が暗号化して他方に送るステップを有することを特徴とする請求項 5 9 記載の情報記録／再生方法。

【請求項 7 5】 データの記録時に、情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いた鍵共有プロトコルを実行するステップと、共有された鍵を用いてデータを情報記録／再生装置が暗号化して他方に送るステップと、セキュリティモジュールが受信したデータを共有された鍵を用いて復号するステップと、セキュリティモジュールが上記復号したデータを鍵を用いて暗号化するステップと、セキュリティモジュールが上記暗号化したデータを情報記録媒体に格納するステップを有することを特徴とする請求項 5 9 記載の情報記録／再生方法。

【請求項 7 6】 データの再生時に、情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いた鍵共有プロトコルを行って鍵を共有するステップと

セキュリティモジュールが情報記録媒体からデータを読み出して鍵を用いて復号するステップと、セキュリティモジュールが上記復号後のデータを共有した鍵を用いて暗号化するステップと、セキュリティモジュールが上記暗号化後のデータを情報記録／再生装置に送信するステップとを有することを特徴とする請求項 5 9 記載の情報記録／再生方法。

【請求項 7 7】 外部装置とインターフェースをとるためのインターフェース機能と、乱数を生成するための乱数生成機能と、情報を保存するための記憶機能と、公開鍵暗号技術を用いた相互認証プロトコルに必要な計算を行う演算機能を有するセキュリティモジュールを備えることを特徴とする情報記録媒体。

【請求項 7 8】 上記セキュリティモジュールは、データを記録するための記録領域にアクセスするためのインターフェース機能を備えることを特徴とする請求項 7 7 記載の情報記録媒体。

【請求項 7 9】 セキュリティモジュールを有する情報記録媒体を製造する記録媒体製造装置であって、

最新のリボケーションリスト及び／又はレジストレーションリストを上記情報記録媒体に記録する記録手段を備える

ことを特徴とする記録媒体製造装置。

【請求項 8 0】 上記情報記録媒体のセキュリティモジュールが上記リボケーションリスト及び／又はレジストレーションリストを保持するのに十分な保持手段を備えるとき、

上記記録手段は、上記保持手段に上記最新のリボケーションリスト及び／又はレジストレーションリストを記録することを特徴とする請求項 7 9 記載の記録媒体製造装置。

【請求項 8 1】 上記情報記録媒体のセキュリティモジュールが上記リボケーションリスト及び／又はレジストレーションリストを保持するのに十分な保持手段を備えないとき、

上記記録手段は、上記情報記録媒体のデータ記録領域に上記最新のリボケーションリスト及び／又はレジストレーションリストを記録することを特徴とする請求項 7 9 記載の記録媒体製造装置。

【請求項 8 2】 上記最新のリボケーションリスト及び／又はレジストレーションリストを格納する格納手段を備えることを特徴とする請求項 7 9 記載の記録媒体製造装置。

【請求項 8 3】 外部から上記最新のリボケーションリスト及び／又はレジストレーションリストを入手する入手手段を備えることを特徴とする請求項 7 9 記載の記録媒体製造装置。

【請求項 8 4】 セキュリティモジュールを有する情報記録媒体を製造する記録媒体製造方法であって、

最新のリボケーションリスト及び／又はレジストレーションリストを上記情報記録媒体に記録するステップを有する

ことを特徴とする記録媒体製造方法。

【請求項 8 5】 上記情報記録媒体のセキュリティモジュールが上記リボケーションリスト及び／又はレジストレーションリストを保持するのに十分な保持手段を備えるとき、

上記保持手段に上記最新のリボケーションリスト及び／又はレジストレーションリストを記録することを特徴とする請求項 8 4 記載の記録媒体製造方法。

【請求項 8 6】 上記情報記録媒体のセキュリティモジュールが上記リボケーションリスト及び／又はレジストレーションリストを保持するのに十分な保持手段を備えないとき、

上記情報記録媒体のデータ記録領域に上記最新のリボケーションリスト及び／又はレジストレーションリストを記録することを特徴とする請求項 8 4 記載の記録媒体製造方法。

【請求項 8 7】 上記最新のリボケーションリスト及び／又はレジストレーションリストを格納するステップを有することを特徴とする請求項 8 4 記載の記録媒体製造方法。

【請求項 8 8】 外部から上記最新のリボケーションリスト及び／又はレジストレーションリストを入手するステップを有することを特徴とする請求項 8 4 記載の記録媒体製造方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、安全にデータを授受することを可能にした情報記録／再生システム、情報記録／再生装置及び方法、情報記録媒体、記録媒体製造装置及び方法に関する。

【0 0 0 2】

【従来の技術】

近年は、情報をデジタル的に記録する記録装置及び記録媒体が普及しつつある。これらの記録装置及び記録媒体は、例えば、映像や音楽のデータを劣化させることなく記録し、再生するので、データを、その質を維持しながら何度もコピーすることができる。しかしながら、映像や音楽のデータの著作権者にしてみれば、自らが著作権を有するデータが、その質を維持しながら何度も不正にコピーされ、市場に流通してしまう恐れがある。このため、記録装置及び記録媒体の側で、著作権を有するデータが不正にコピーされるのを防ぐ必要がある。

【0 0 0 3】

このような著作権保護のための手法として、例えば、ミニディスク（MD）（商

標) システムにおいては、いわゆる SCMS (Serial Copy Management System) と呼ばれる方法が用いられている。当該 SCMS の情報は、デジタルインターフェースによって、音楽データとともに伝送される情報であり、この情報は、音楽データがコピーフリー (以下、copy free と記す) であるか、又は、1 回のみコピーを許す (以下、copy once allowed と記す) データであるか、コピーが禁止されている (以下、copy prohibited と記す) データであるかのうちのいずれのデータであるのかを表す。ミニディスクレコーダは、デジタルインターフェースから音楽データを受信した場合、上記 SCMS の情報を検出し、これが copy prohibited であれば、音楽データをミニディスクに記録せず、copy once allowed であれば、当該 SCMS の情報を copy prohibited に変更して受信した音楽データとともに記録し、copy free であれば、当該 SCMS の情報をそのまま、受信した音楽データとともに記録する。

【0004】

このように、ミニディスクシステムにおいては、SCMS の情報を用いて、著作権を有するデータが不正にコピーされるのを防いでいる。

【0005】

また、著作権を有するデータが不正にコピーされるのを防ぐ別の例としては、デジタルバーサタイルディスク (Digital Versatile Disk: DVD (商標)) システムにおける、コンテンツスクランブルシステムが挙げられる。このシステムでは、ディスク上の著作権を有するデータが全て暗号化され、ライセンスを受けた記録装置だけが暗号鍵を与えられ、これにより上記暗号化されているデータを復号し、意味のあるデータを得ることができるようになされている。そして、記録装置は、ライセンスを受ける際に、不正コピーを行わない等の動作規定に従うように設計される。このようにして、DVD システムにおいては、著作権を有するデータが不正にコピーされるのを防いでいる。

【0006】

【発明が解決しようとする課題】

しかしながら、上記のミニディスクシステムが採用している方式では、SCMS が copy once allowed であれば、これを copy prohibited に変更し、受信したデ

ータとともに記録するなどの動作規定に従わない記録装置が、不正に製造されてしまう虞がある。

【 0 0 0 7 】

また、上記のDVDシステムが採用している方式では、再生のみ可能なROMメディアに対しては有効であるが、ユーザがデータを記録可能なRAMメディアにおいては有効ではない。すなわち、RAMメディアにおいては、不正者は、暗号を解読できない場合であっても、ディスク上のデータを全部、新しいディスクに不正にコピーすることによって、ライセンスを受けた正当な記録装置で動作するディスクを新たに作ることができるからである。

【 0 0 0 8 】

このようなことから、本件出願人は、先に出願した特願平 1 0 - 2 5 3 1 0 号の特許出願において、個々の記録媒体を識別するための情報（以下、媒体識別情報と呼ぶ）を記録媒体に持たせ、この情報はライセンスを受けた装置しかアクセスできないようにすることにより、不正コピーを防止する技術を提案している。すなわち、当該技術においては、記録媒体上のデータを、ライセンスを受けることによって得られる秘密に基づく鍵と媒体識別情報の両方を用いて暗号化することにより、ライセンスを受けていない装置がデータを読み出しても意味のないものとしている。さらに、当該技術によれば、装置にライセンスを与える際にその装置の動作を規定し、不正コピーを行わないようにもしている。このように、上記技術によれば、ライセンスを得ていない装置は媒体識別情報にアクセスできず、また媒体識別情報は個々の媒体毎に個別の値になっているため、例えばライセンスを受けていない装置がアクセス可能なすべての情報を新たな媒体にコピーしたとしても、そのようにして作られた媒体は、ライセンスを受けていない装置でもライセンスを受けた装置でも正しく情報が読み出せないことになり、不正コピーの防止が実現されている。

【 0 0 0 9 】

しかしながら、上記技術においては、ある記録装置によって情報が記録された記録媒体を他の装置にて再生できることを保証するために、記録媒体上のデータを暗号化するための暗号鍵は、システム全体で共通の秘密鍵（マスターキー）に

基づいて生成されるようになっている。これはすなわち、例えば正当な一つの装置が解析されて不正にマスターキーが盗まれてしまうようなことが起きると、そのシステムの任意の装置によって記録されたすべてのデータの暗号が解かれ、システム全体が壊滅する恐れがあることを意味している。

【0010】

そこで、本発明の目的は、暗号鍵を安全に保管することができるようにした情報記録／再生システム、情報記録／再生装置、情報記録／再生方法、情報記録媒体、及び情報記録媒体製造装置及び方法を提供することにある。

【0011】

また、本発明の他の目的は、不正な機器にデータを漏らすことのないように、
或いは正当な機器のみにデータを供給できるようにした情報記録／再生システム、情報記録／再生装置及び方法、情報記録媒体、記録媒体製造装置及び方法を提供することにある。

【0012】

また、本発明の他の目的は、正当な機器ではあるが、例えば不正な解析により当該機器の秘密が露呈してしまったような場合に、当該機器に対して新たにデータを与えてしまうことをも防ぐことができるようにした、情報記録／再生システム、情報記録／再生装置及び方法、情報記録媒体、記録媒体製造装置及び方法を提供することにある。

【0013】

さらに、本発明の他の目的は、映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことができるようにした情報記録／再生システム、情報記録／再生装置及び方法、情報記録媒体、記録媒体製造装置及び方法を提供することにある。

【0014】

【課題を解決するための手段】

本発明では、情報記録媒体にセキュリティモジュールを持たせる。情報記録媒体上に記録されるデータは、個々のデータ毎に異なる暗号鍵で暗号化され、暗号鍵はセキュリティモジュールが安全に保管する。また、セキュリティモジュール

は記録／再生装置と公開鍵暗号技術を用いた相互認証を行い、相手が正当なライセンスを受けた装置であることを確認した上で、暗号鍵を装置に対して与えることにより、不正な装置にはデータを漏らさないようにする。さらに、信頼できるセンタが発行するリボケーションリスト及び／又はレジストレーションリストを活用することにより、正当な機器ではあるが不正な解析によって当該機器の秘密が露呈してしまったような場合に、その装置に新たにデータを与えてしまうことをも防ぐことができるようにする。

【0015】

すなわち、本発明に係る情報記録／再生システムは、セキュリティモジュールを有する情報記録媒体と、上記セキュリティモジュールが管理する暗号鍵によって暗号化されたデータを上記情報記録媒体に記録、あるいは、上記セキュリティモジュールが管理する暗号鍵によって暗号化されたデータを上記情報記録媒体から再生する情報記録／再生装置とを備え、情報記録時、又は情報再生時に上記情報記録／再生装置とセキュリティモジュールとが公開鍵暗号技術を用いた相互認証プロトコルを実行することにより、上述した課題を解決する。

【0016】

また、本発明に係る情報記録媒体は、データの記録時及び再生時に、情報記録／再生装置との間で公開鍵暗号を用いた相互認証プロトコルを実行するセキュリティモジュールを有することにより、上述した課題を解決する。

【0017】

また、本発明に係る情報記録／再生装置は、データの記録時及び再生時に、情報記録媒体のセキュリティモジュールとの間で公開鍵暗号を用いた相互認証プロトコルを実行する制御手段を備えることにより、上述した課題を解決する。

【0018】

また、本発明は、情報記録／再生装置により情報記録媒体にデータを記録、あるいは情報記録媒体からデータを再生する情報記録／再生方法において、情報記録媒体が有するセキュリティモジュールと情報記録／再生装置が公開鍵暗号を用いた相互認証プロトコルを実行するステップを有することにより、上述した課題を解決する。

【0019】

さらに、本発明に係る情報記録媒体は、外部装置とインターフェースをとるためのインターフェース機能と、乱数を生成するための乱数生成機能と、情報を保存するための記憶機能と、公開鍵暗号技術を用いた相互認証プロトコルに必要な計算を行う演算機能を有するセキュリティモジュールを備えることにより、上述した課題を解決する。

【0020】

また、本発明の記録媒体製造装置は、セキュリティモジュールを有する情報記録媒体を製造する記録媒体製造装置であって、最新のリボケーションリスト及び／又はレジストレーションリストを上記情報記録媒体に記録する記録手段を備えることにより、上述した課題を解決する。

【0021】

また、本発明の記録媒体製造方法は、セキュリティモジュールを有する情報記録媒体を製造する記録媒体製造方法であって、最新のリボケーションリスト及び／又はレジストレーションリストを上記情報記録媒体に記録するステップを有することにより、上述した課題を解決する。

【0022】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら詳細に説明する。

【0023】

図1には、本発明の第1の実施の形態に係る情報記録媒体の一例としての光ディスク情報記録媒体10の構成例を示す。

【0024】

この光ディスク情報記録媒体10は、カートリッジ11内に、データを記録する光ディスク12と、不揮発性メモリ34を有するセキュリティモジュール13とを備えている。図2は、当該第1の実施の形態において不揮発性メモリ34を有するセキュリティモジュール13の構成例を示している。

【0025】

セキュリティモジュール13は、図2に示すように、当該モジュール外の装置

とデータの授受をするための接触式あるいは非接触式のインターフェース部 3 1 と、各種の演算を行うための演算部 3 2 と、乱数発生部 3 3 と、不揮発性メモリ 3 4 と、それらを制御するための制御部 3 5 とを備えている。

【 0 0 2 6 】

図 3 は、本発明の第 1 の実施の形態としての光ディスク記録再生装置 1 0 0 の構成例を示している。

【 0 0 2 7 】

この光ディスク記録再生装置 1 0 0 は、上記光ディスク情報記録媒体 1 0 を使用してデータの記録／再生を行うものであり、カートリッジ 1 1 内の光ディスク 1 2 を回転させるスピンドルモータ 1 0 1、光学ヘッド 1 0 2、サーボ回路 1 0 3、記録／再生回路 1 0 4、これらを制御する制御部 1 0 5、この制御部 1 0 5 に接続された入力部 1 0 6、乱数を発生する乱数発生部 1 0 7、不揮発性メモリ 1 1 0、インターフェース部 1 0 8 などを備えている。

【 0 0 2 8 】

スピンドルモータ 1 0 1 は、サーボ回路 1 0 3 によってその回転動作が制御され、光ディスク 1 2 を回転させる。光学ヘッド 1 0 2 は、レーザビームを光ディスク 1 2 の記録面に照射することで、データの記録／再生を行う。サーボ回路 1 0 3 は、スピンドルモータ 1 0 1 を駆動することにより、光ディスク 1 2 を所定の速度で（例えば線速度一定で）回転させる。また、サーボ回路 1 0 3 は、光学ヘッド 1 0 2 による光ディスク 1 2 へのトラッキング及びフォーカシングの他、上記光学ヘッド 1 0 2 をディスク半径方向に移動させる際のスレッドサーボ制御を行う。

【 0 0 2 9 】

そして、記録／再生回路 1 0 4 は、制御部 1 0 5 により動作モードが切り換えられる暗号化部 1 0 4 A と復号部 1 0 4 B を有する。暗号化部 1 0 4 A は、記録モード時に、外部から記録信号の供給を受けると、その記録信号を暗号化し、光学ヘッド 1 0 2 に供給して、光ディスク 1 2 に記録させる。復号部 1 0 4 B は、再生モード時に、光学ヘッド 1 0 2 により光ディスク 1 2 から再生されたデータを復号し、外部に再生信号として出力する。

【0030】

また、入力部106は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作がなされたとき、その入力操作に対応する信号を出力する。制御部105は、記憶されている所定のコンピュータプログラムに従って、装置全体を制御する。乱数発生部107は、制御部105の制御により、所定の乱数を発生する。インターフェース108部は、接触式あるいは非接触式であり、情報記録媒体10のセキュリティモジュール13との間でデータの授受を行う。

【0031】

さらに、この第1の実施の形態の光ディスク記録再生装置100は、演算部109と不揮発性メモリ110を備えている。

【0032】

ここで、本発明の第1の実施の形態において、上記光ディスク情報記録媒体10のセキュリティモジュール13は、個別の(1つの媒体毎)識別コード(ID)と、当該IDに対応する公開鍵暗号系の秘密鍵と公開鍵、さらに信頼できるセンタ(Trusted Center:TC、以下、単にセンタTCと呼ぶ)から公開鍵証明書が与えられており、それら情報を不揮発性メモリ34或いは当該不揮発性メモリ34とは別の不揮発性の記憶領域に格納している。同じく、この第1の実施の形態の光ディスク記録再生装置100は、個別の(1台の装置毎の)識別コード(ID)と、当該IDに対応する公開鍵暗号系の秘密鍵と公開鍵、センタTCから公開鍵証明書が与えられており、これら情報を不揮発性メモリ110或いは当該不揮発性メモリ110とは別の不揮発性の記憶領域に格納している。特に、秘密鍵は外部に漏れないように、それぞれ不揮発性メモリ34、110或いはそれらとは別の記憶領域において安全に格納する。

【0033】

上記光ディスク情報記録媒体10のセキュリティモジュール13に与えられている上記公開鍵証明書は、当該光ディスク情報記録媒体10のIDと公開鍵を含む情報に、センタTCがデジタル署名を施したデータである。同様に、光ディスク記録再生装置100に与えられている公開鍵証明書は、当該光ディスク記録再

生装置 1 0 0 の ID と公開鍵を含む情報に、センタ TC がデジタル署名を施したデータである。すなわち、これら公開鍵証明書は、個々の光ディスク情報記録媒体、及び、個々の光ディスク記録再生装置が、それぞれ正当なものであることをセンタ TC が認めることを証明する文書であり、通常は、各記録媒体、装置がそれぞれ出荷される時に、センタ TC から与えられるものである。なお、上記デジタル署名技術とは、あるデータを生成したのが、あるユーザであることを証明できる技術であり、例えば IEEE P 1 3 6 3 で使用されているいわゆる EC - DSA (Elliptic Curve Digital Signature Algorithm) 方式などがよく知られている。

【 0 0 3 4 】

上記公開鍵証明書には、図 4 に示すように、エンティティ ID (Entity ID)、エンティティ公開鍵 (Entity Public Key)、センタ TC のデジタル署名の各項目が含まれる。なお、上記エンティティ (Entity) とは、本発明実施の形態の情報記録媒体または記録再生装置を指す。上記エンティティ ID はそのエンティティに個別に与えられた識別番号である。また、各エンティティには、公開鍵と秘密鍵のペアも個別に与えられ、そのうち公開鍵は上記公開鍵証明書に書かれ、秘密鍵はそのエンティティが秘密に保持する。また、エンティティタイプ (Entity Type) とは、情報記録媒体又は記録再生装置が後述するリボケーションリスト (或いは後の第 2 の実施の形態で説明するレジストレーションリスト) 等を格納するための不揮発性メモリを備えたタイプであるか、或いは当該リストを格納するための不揮発性メモリを備えていないタイプであるかや、記録媒体の物理的構造を区別するための識別符号である。

【 0 0 3 5 】

また、この第 1 の実施の形態において、光ディスク情報記録媒体 1 0 の不揮発性メモリ 3 4 と光ディスク記録再生装置 1 0 0 の不揮発性メモリ 1 1 0 には、それぞれ上記公開鍵証明書に含まれる上記センタ TC のデジタル署名を検証するために、システム全体で共通であるセンタ TC の公開鍵がそれぞれ格納されている。

【0036】

さらに、当該第1の実施の形態において、光ディスク情報記録媒体10のセキュリティモジュール13の不揮発性メモリ34と、光ディスク記録再生装置100の不揮発性メモリ110には、図5に示すリボケーションリストを格納する領域がそれぞれ設けられている。

【0037】

上記リボケーションリストは、単調増加する番号であって当該リボケーションリストのバージョンを示すバージョンナンバーと、秘密鍵が露呈してしまった光ディスク情報記録媒体或いは光ディスク記録再生装置のID（リボークされる機器又は媒体のID）のリストと、センタTCによるデジタル署名とからなるものである。すなわち、リボケーションリストは、不正者リスト或いはブラックリストとも呼ばれ、本実施の形態のような光ディスク情報記録媒体や光ディスク記録再生装置等から成るシステム全体においてその記録媒体又は装置の秘密鍵が露呈してしまったものIDがリストアップされ、それに対し信頼できるセンタTCがデジタル署名を施したものである。したがって、あるエンティティ（情報記録媒体または記録再生装置）において、通信相手方の記録媒体若しくは装置のIDが当該リボケーションリストに載っていることを確認した場合、そのエンティティは通信相手方を不正なものと判断し、それ以上プロトコルを進めないようにすることができる。このことにより、秘密鍵が露呈してしまった記録媒体又は装置、及びそれを用いて不正に複製された記録媒体又は不正に製造された装置を、このシステムから排除することが可能になる。また、光ディスク記録再生装置100を工場から出荷する際には、最新版のリボケーションリストを不揮発性メモリ110に格納して出荷する。

【0038】

次に、図6から図8を用いて、第1の実施の形態の光ディスク記録再生装置100が光ディスク情報記録媒体10にデータを記録する手順を説明する。

【0039】

なお、上述したように、第1の実施の形態の光ディスク記録再生装置100は、センタTCから与えられたID、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明

書、及びリボケーションリストを上記不揮発性メモリ 110 に格納しており、また同様に、当該第 1 の実施の形態の光ディスク情報記録媒体 10 のセキュリティモジュール 13 は、センタ TC から与えられた ID、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを上記不揮発性メモリ 34 に格納している。

【0040】

先ず、図 6 において、光ディスク記録再生装置 100 は、手順 R1 として、光ディスク情報記録媒体 10 のセキュリティモジュール 13 に対して、これからデータの記録を行うことを示す記録コマンド（記録開始コマンド）と、1 回 1 回の記録を識別するために個別に割り当てるレコーディング ID（Recording-ID）とを送る。

【0041】

次に、手順 R2 として、光ディスク記録再生装置 100 及び光ディスク情報記録媒体 10 のセキュリティモジュール 13 は、上記記録コマンドをトリガーとして、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する。

【0042】

ここで、公開鍵暗号技術を用いた相互認証プロトコルは、相手側が正しい（センタ TC から承認を得た）公開鍵と秘密鍵のペアを持っていることを互いに確認するプロトコルであり、例えば IEEE P1363 で規格化作業中の ECDSA（Elliptic Curve Digital Signature Algorithm）を用いることによって構成することができる。

【0043】

なお、上記公開鍵暗号技術を用いた相互認証プロトコルにおいては、光ディスク情報記録媒体 10 のセキュリティモジュール 13 と光ディスク記録再生装置 100 の双方が、それぞれ乱数発生機能（セキュリティモジュール 13 の乱数発生部 33、装置 100 の乱数発生部 107）を用いて乱数を発生させること、不揮発性メモリに格納されている自己の秘密鍵及び公開鍵証明書を読み出すこと、公開鍵暗号技術に基づく演算を演算機能（演算部）で行うこと、が必要となる。

【 0 0 4 4 】

また、公開鍵暗号技術を用いた相互認証プロトコルに対し、共通鍵暗号技術を用いた相互認証プロトコルも広く知られているが、当該相互認証プロトコルはその名の通り、プロトコルを実行する 2 者が共通の鍵を持っていることを前提とするプロトコルである。共通鍵暗号技術を用いた相互認証プロトコルを採用しようとした場合、記録媒体と記録再生装置のインターオペラビリティを確保する必要があるため、システム全体で共通の鍵をすべてのセキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 が持つ必要がある。但し、この場合、一つのセキュリティモジュールあるいは光ディスク記録再生装置が攻撃を受けて（解析されて）鍵が露呈してしまうと、その影響がシステム全体に広まってしまうという問題がある。

【 0 0 4 5 】

これに対し、公開鍵暗号技術を用いた相互認証プロトコルにおいては、各装置及び各セキュリティモジュールが持つ鍵は個別であり、しかも本実施の形態では上述したリボケーションリストを使用できるため、一つの装置或いは記録媒体の鍵が露呈したとしても、その装置或いは記録媒体だけをシステムから排除することができるので、影響を小さく抑えられるという利点がある。

【 0 0 4 6 】

上記公開鍵暗号技術を用いた鍵共有プロトコルは、2 者間で安全に秘密情報を共有するためのプロトコルであり、やはり I E E E P 1 3 6 3 で規格化作業中のいわゆる E C - D H (Elliptic Curve Diffie Hellman) を用いることによって構成することができる。

【 0 0 4 7 】

公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実際に用いている例としては、I E E E 1 3 9 4 パス上のコンテンツプロテクション方式の一つである、ソニー、松下、日立、東芝、インテルの 5 社によって開発された、いわゆる D T C P (Digital Transmission Content Protection) 規格（この規格そのものはライセンスを受けないと見ることができないが、その概要を記した White Paper 或いは規格の Informational version を、ライセンス組織であるいわゆる D

T L A (Digital Transmission Licensing Administrator) のウェブページである <http://www.dtcp.com> から誰でも取得することが可能である) の F A K E (Full Authentication and Key Exchange) プロトコルを挙げることができる。このプロトコルは、おおまかには下記のステップで構成される。

【 0 0 4 8 】

すなわち、当該プロトコルでは、先ず第 1 のステップとして、乱数発生器を用いて乱数を発生させ、不揮発性メモリから読み出した自分の公開鍵証明書とともに他方に送る。

【 0 0 4 9 】

次に、当該プロトコルでは、第 2 のステップとして、相手の公開鍵証明書の正当性を公開鍵暗号技術に基づく演算を行って確かめる。

【 0 0 5 0 】

次に、当該プロトコルでは、第 3 のステップとして、鍵共有のための、公開鍵暗号技術に基づく演算（第 1 段階）を行い、公開鍵暗号技術に基づく演算を行って作成した自分のデジタル署名文とともに相手に送る。

【 0 0 5 1 】

その後、当該プロトコルでは、第 4 のステップとして、相手から送られた第 3 のステップでのデータについて、公開鍵暗号技術に基づく演算を行って相手のデジタル署名の検証を行い、鍵共有のための、公開鍵暗号技術に基づく演算（第 2 段階）を行って共有鍵の値を計算する。

【 0 0 5 2 】

本方式においては、上記相互認証を行う際に、相手の装置が正しい秘密鍵と公開鍵のペアを持っていることのみならず、自分が持つリボケーションリストに相手の装置の ID が掲載されていないことを確認する。すなわち、出荷時には正當に鍵を持っていたが、それが例えばいわゆるリバースエンジニアリングなどの攻撃（不正な解析）を受け、鍵が露呈してしまった装置の ID が上記リボケーションリストに載せられているような場合には、当該リボケーションリストに載せられている装置（データを渡してはいけない装置）に対してデータを渡さずに済むようになる。

【0053】

図6に戻り、さらに、上記手順R2では、記録再生装置と記録媒体のセキュリティモジュールとの間で、それぞれ自分が持っているリボケーションリストのバージョンナンバーを交換する。

【0054】

次に、手順R3、R4として、もし何れかの一方が他方のリボケーションリストより新しいリボケーションリストを持っていた場合、当該新しいリボケーションリストを持っている方は自分のリボケーションリストを他方に送る。一方、古いリボケーションリストを持っている方は、新しいリボケーションリストを持っている方から、当該新しいリボケーションリストを送ってもらい、その正当性を検証した後、自分が持つリボケーションリストを、その送られてきた新しいリボケーションリストに更新する。すなわち、手順R3には、セキュリティモジュール上のリボケーションリストのバージョンが、記録再生装置上のリボケーションリストのバージョンよりも新しい場合におけるリボケーションリストの流れを示しており、また、手順R4には、記録再生装置上のリボケーションリストのバージョンが、セキュリティモジュール上のリボケーションリストのバージョンよりも新しい場合におけるリボケーションリストの流れを示している。

【0055】

なお、手順R3、R4におけるリボケーションリストの送付は、後の手順R5におけるデータの記録と順序が前後してもかまわない。つまり、手順R5にてデータの記録を行った後に、手順R3或いはR4でのリボケーションリストの送付を行うようにしてもよい。

【0056】

さてここで、上述したような公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルの結果、光ディスク記録再生装置100とセキュリティモジュール13は、安全に、ある値を共有することになる。以下、この共有される値をセッション鍵 (Session key: Kse) と呼ぶことにする。

【0057】

次に、データを暗号化する暗号鍵 (Content key: Kco) を決定するが、その決

定方法としては、例えば、以下に述べる暗号鍵決定方法（１）～暗号鍵決定方法（２）のうちの一つを用いればよい。

【００５８】

暗号鍵決定方法（１）では、 $K_{se}=K_{co}$ とする。すなわち、セッション鍵 K_{se} を暗号鍵 K_{co} とする。この時、セキュリティモジュール１３は、暗号鍵 K_{co} を安全にその内部の不揮発性メモリ３４に格納するか、セキュリティモジュール１３が予め格納しているストレージ鍵（Storage key: K_{st} ）を用いて当該暗号鍵 K_{co} を暗号化した値 $E_{nc}(K_{st}, K_{co})$ を光ディスク記録再生装置１００に送り、光ディスク１２に記録させる。

暗号鍵決定方法（２）では、セキュリティモジュール１３が予め格納しているストレージ鍵 K_{st} を暗号鍵 K_{co} とする。この場合、セキュリティモジュール１３がストレージ鍵 K_{st} を上記セッション鍵 K_{se} で暗号化して光ディスク記録再生装置１００に送り、ストレージ鍵 $K_{st}(=k_{co})$ を用いてデータを暗号化して光ディスク１２に記録させる。

暗号鍵決定方法（３）では、セキュリティモジュール１３がそのデータ用の暗号鍵 K_{co} を乱数発生器などを用いて新たに発生させる。この場合、セキュリティモジュール１３が当該暗号鍵 K_{co} を上記セッション鍵 K_{se} で暗号化して光ディスク記録再生装置１００に送り、この装置１００において当該暗号鍵 K_{co} を用いてデータを暗号化して光ディスク１２に記録させる。セキュリティモジュール１３は、暗号鍵 K_{co} を安全にその内部の不揮発性メモリ３４に格納するか、セキュリティモジュール１３が予め格納しているストレージ鍵 K_{st} を用いて上記暗号鍵 K_{co} を暗号化した値 $E_{nc}(K_{st}, K_{co})$ を光ディスク記録再生装置１００に送り、光ディスク１２に記録させる。

暗号鍵決定方法（４）では、光ディスク記録再生装置１００がそのデータ用の暗号鍵 K_{co} を乱数発生器などを用いて新たに発生させ、当該暗号鍵 K_{co} によりデータを暗号化して記録する。この場合、光ディスク記録再生装置１００が暗号鍵 K_{co} をセッション鍵 K_{se} で暗号化してセキュリティモジュール１３に送る。セキュリティモジュール１３は暗号鍵 K_{co} を安全にその内部の不揮発性メモリ３４に格納するか、セキュリティモジュール１３が予め格納しているストレージ鍵 K_{st}

を用いて暗号鍵 K_{co} を暗号化した値 $E_{nc}(K_{st}, K_{co})$ を光ディスク記録再生装置 100 に送り、光ディスク 13 に記録させる。

【0059】

上述した暗号鍵決定方法 (1) ~ (4) の何れかを用いて暗号鍵 K_{co} を決定したならば、次に、手順 R5 として、光ディスク記録再生装置 100 は、光ディスク 12 に記録するデータを当該暗号鍵 K_{co} で暗号化し、その暗号化されたデータ $E_{nc}(K_{co}, data)$ を光ディスク 12 に記録する。

【0060】

また、上記暗号化 K_{co} 、又は暗号化した暗号鍵 K_{co} を、セキュリティモジュール 13 の不揮発性メモリ 34 に記録する際には、レコーディング ID (Recording-ID) を検索用のキーとするために一緒に記録したり、データが記録される光ディスク 12 のセクタと同一のセクタに暗号化した K_{co} を記録するなどして、データと暗号鍵 K_{co} の対応がとれるようにしておく。なお、この暗号鍵 K_{co} の管理、伝送と、データの暗号化には、その処理速度の観点から共通鍵暗号アルゴリズムを使用することが好適である。

【0061】

共通鍵暗号アルゴリズムは、暗号化とその復号の処理に同一の暗号鍵を用いる暗号アルゴリズムであり、FIPS 46-2 で米国の標準に指定されているいわゆる DES (Data Encryption Standard) をその例として挙げることできる。

【0062】

特に、上記暗号鍵決定方法 (4) の場合には、光ディスク記録再生装置 100 が暗号鍵 K_{co} を決められるため、光ディスク記録再生装置 100 は予めデータを暗号化しておくことが可能になる。

【0063】

当該第 1 の実施の形態では、以上の手順により、データを光ディスク 12 に記録する。

【0064】

次に、図 7 には、上記図 6 に示した第 1 の実施の形態の光ディスク記録再生装置 100 が光ディスク情報記録媒体 10 にデータを記録するまでの手順の詳細を

示す。なお、この図7では、光ディスク記録再生装置100に係る各情報について「B」の文字を付し、光ディスク情報記録媒体10のセキュリティモジュール13に係る各情報について「A」の文字を付している。また、図6で説明したのと同様に、光ディスク記録再生装置100とセキュリティモジュール13は、センタTCから与えられたID（セキュリティモジュール13のID_A、光ディスク記録再生装置100のID_B）、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを、それぞれ対応する不揮発性メモリ110、34に格納している。

【0065】

図7において、先ず、光ディスク記録再生装置100は、手順R11として、前記乱数発生部107にて64ビットの乱数R_Bを生成し、この乱数R_Bを記録コマンド（記録開始コマンド）と共にセキュリティモジュール13に送る。

【0066】

上記記録コマンドと乱数R_Bを受け取ったセキュリティモジュール13は、手順R12として、前記乱数発生部33にて64ビットの乱数R_Aを発生すると共に、当該セキュリティモジュール13から外部に出力されることのない秘密の所定値或いは乱数のK_A（ $0 < K_A < r$ ）を生成し、前記EC-DHアルゴリズムの第1段階（ステップ1）においてphase 1 value V_Aの値を計算（ $V_A = K_A \cdot G$ ）により求める。なお、 $V_A = K_A \cdot G$ は、いわゆる楕円関数を用いた暗号技術における楕円曲線上の演算であり、Gは楕円曲線上のある点を表し、システムにおいて共通に設定されている値である。また、rは楕円関数の位数である。更に、セキュリティモジュール13は、前記EC-DSAの署名アルゴリズムを用いて、上記乱数R_A、乱数R_B、値V_A、リボケーションリストのバージョンナンバーRevV_Aからなるビット列R_A||R_B||V_A||RevV_Aにデジタル署名の関数Signを用いたデジタル署名を行い $Sig_A = \text{Sign}(\text{PriKey}_A, R_A || R_B || V_A || \text{Rev}V_A)$ を得る。なお、PriKey_Aはセキュリティモジュール13のプライベート鍵であり、「||」はビットの連結を表している。セキュリティモジュール13は、これらR_A、R_B、V_A、RevV_A、Sig_Aに証明書Cert_Aを付け、光ディスク記録再生装置100に送る。なお、セキュリティモジュール13がリボケーションリストを持

たない場合或いは使用しない場合は、当該バージョンナンバーとして0を用いる。

【0067】

上記セキュリティモジュール13から $Cert_A$, R_A , R_B , V_A , $RevV_A$, Sig_A を受け取ると、光ディスク記録再生装置100は、ECDSAの証明アルゴリズムを用いて、セキュリティモジュール13の証明書 $Cert_A$ 、デジタル署名 Sig_A 、 ID_A の検証（チェック）を行う。

【0068】

すなわち、光ディスク記録再生装置100は、先ず、セキュリティモジュール13の証明書 $Cert_A$ の検証を行い、例えば当該検証をパスできないときには、そのセキュリティモジュール13を備えた光ディスク情報記録媒体10を不正な媒体とみなして当該プロトコルを終了する。

【0069】

一方、セキュリティモジュール13の証明書 $Cert_A$ の検証において正当であると判定された場合、光ディスク記録再生装置100は、上記証明書 $Cert_A$ からパブリック鍵 $PubKey_A$ を手に入れる。次に、光ディスク記録再生装置100は、セキュリティモジュール13から返送されてきた乱数 R_B と、当該光ディスク記録再生装置100が手順R11で生成した乱数 R_B とが等しく、さらに上記デジタル署名 Sig_A が正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール13を備えた光ディスク情報記録媒体10が不正な媒体であると判断して当該プロトコルを終了する。

【0070】

上述のように、セキュリティモジュール13から返送された乱数 R_B が先に生成したものと等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、光ディスク記録再生装置100は、自己の不揮発性メモリ110に格納しているリボケーションリストを用い、セキュリティモジュール13を備えた光ディスク情報記録媒体10の ID_A が当該リボケーションリストに掲載されていないことを検証する。この検証の結果、セキュリティモジュール13を備えた光ディスク情報記録媒体10の ID_A がリボケーションリストに掲載されている場合には、

当該セキュリティモジュール 13 を備えた光ディスク情報記録媒体 10 は不正な媒体であると判定し、当該プロトコルを終了する。

【0071】

一方、セキュリティモジュール 13 を備えた光ディスク情報記録媒体 10 の ID_A が当該リボケーションリストに掲載されておらず、その光ディスク情報記録媒体 10 が正当であると判断した場合、光ディスク記録再生装置 100 は、手順 R13 として、当該装置 100 から外部に出力されることのない秘密の所定値或いは乱数の K_B ($0 < K_B < r$) を生成し、前記 EC-DH アルゴリズムの第 1 段階 (ステップ 1) において $pahe$ se 1 value V_B 値を計算 ($V_B = K_B \cdot G$) により求める。更に、光ディスク記録再生装置 100 は、前記 EC-DSA の署名アルゴリズムを用いて、上記乱数 R_B 、乱数 R_A 、値 V_B 、当該装置 100 が持つリボケーションリストのバージョンナンバー $RevV_B$ からなるビット列 $R_B || R_A || V_B || RevV_B$ にデジタル署名の関数 $Sign$ を用いたデジタル署名を行い $Sig_B = Sign(PriKey_B, R_B || R_A || V_B || RevV_B)$ を得る。なお、 $PriKey_B$ は光ディスク記録再生装置 100 のプライベート鍵である。光ディスク記録再生装置 100 は、これら R_B 、 R_A 、 V_B 、 $RevV_B$ 、 Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール 13 に送る。なお、光ディスク記録再生装置 100 がリボケーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして 0 を用いる。

【0072】

上記光ディスク記録再生装置 100 から $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RevV_B$ 、 Sig_B を受け取ると、セキュリティモジュール 13 は、EC-DSA の証明アルゴリズムを用いて、光ディスク記録再生装置 100 の証明書 $Cert_B$ 、デジタル署名 Sig_B 、 ID_B の検証 (チェック) を行う。

【0073】

すなわち、セキュリティモジュール 13 は、先ず、光ディスク記録再生装置 100 の証明書 $Cert_B$ の検証を行い、例えば当該検証をパスできないときには、その光ディスク記録再生装置 100 を不正な装置とみなして当該プロトコルを終了する。

【0074】

一方、光ディスク記録再生装置100の証明書 $Cert_B$ の検証において正当であると判定された場合、セキュリティモジュール13は、上記証明書 $Cert_B$ からパブリック鍵 $PubKey_B$ を手に入れる。次に、セキュリティモジュール13は、光ディスク記録再生装置100から返送されてきた乱数 R_A と、当該セキュリティモジュール13が手順R12で生成した乱数 R_A とが等しく、さらに上記デジタル署名 Sig_B が正当であると判定されたときには、次の処理に進み、そうでない場合には光ディスク記録再生装置100が不正な装置であると判断して当該プロトコルを終了する。

【0075】

上述のように、光ディスク記録再生装置100から返送された乱数 R_A と先に生成したものが等しく、且つデジタル署名 Sig_B が正当であると判定されたとき、セキュリティモジュール13は、自己の不揮発性メモリ34に格納しているリボケーションリストを用い、光ディスク記録再生装置100の ID_B が当該リボケーションリストに掲載されていないことを検証する。この検証の結果、光ディスク記録再生装置100の ID_B がリボケーションリストに掲載されている場合には、当該光ディスク記録再生装置100は不正な装置であると判定し、当該プロトコルを終了する。

【0076】

一方、光ディスク記録再生装置100の ID_B が当該リボケーションリストに掲載されておらず、その光ディスク記録再生装置100が正当であると判断した場合、すなわち、セキュリティモジュール13と光ディスク記録再生装置100の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール13では $K_A \cdot V_B$ の計算を行い、また、光ディスク記録再生装置100では $K_B \cdot V_A$ の計算を行い、さらにそれらのx座標の下位zビットをセッション鍵 K_{se} としてこれらセキュリティモジュール13と光ディスク記録再生装置100が共有する。

【0077】

次に、セキュリティモジュール13と光ディスク記録再生装置100は、それ

ぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順 R 1 4 又は R 1 5 として、その新しいバージョンのリボケーションリストを相手方に送る。すなわち、セキュリティモジュール 1 3 では、光ディスク記録再生装置 1 0 0 が保持しているリボケーションリストのバージョンナンバー $RevV_B$ が、自己のリボケーションリストのバージョンナンバー $RevV_A$ よりも新しいか否かチェックし、 $RevV_A$ が $RevV_B$ よりも新しいとき、手順 R 1 5 として、自己の保持しているリボケーションリストを光ディスク記録再生装置 1 0 0 に送る。一方、光ディスク記録再生装置 1 0 0 では、セキュリティモジュール 1 3 が保持しているリボケーションリストのバージョンナンバー $RevV_A$ が、自己のリボケーションリストのバージョンナンバー $RevV_B$ よりも新しいか否かチェックし、 $RevV_B$ が $RevV_A$ よりも新しいとき、手順 R 1 4 として、自己の保持しているリボケーションリストをセキュリティモジュール 1 3 に送る。

【 0 0 7 8 】

上述のように、相手方から新しいバージョンナンバーのリボケーションリストが送られてきた方は、当該リボケーションリスト内に含まれるセンタ TC の署名 TC Sig を検証し、当該署名 TC Sig が正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新（リストのアップデート）する。一方、署名 TC Sig が正しくない場合は、当該プロトコルを終了する。

【 0 0 7 9 】

その後、光ディスク記録再生装置 1 0 0 は、手順 R 1 6 として、光ディスク 1 2 に記録するコンテンツデータを暗号化するための暗号鍵（コンテンツ鍵） K_{co} を定め、この暗号鍵 K_{co} をセッション鍵 K_{se} にて暗号化した値 $E_{nc}(K_{se}, K_{co})$ をセキュリティモジュール 1 3 に送信する。

【 0 0 8 0 】

セキュリティモジュール 1 3 は、手順 R 1 7 として、上記光ディスク記録再生装置 1 0 0 から送信されてきた値 $E_{nc}(K_{se}, K_{co})$ をセッション鍵 K_{se} を用いて復号することにより、暗号鍵 K_{co} を復元し、さらに、この暗号鍵 K_{co} を自己が持

つストレージ鍵 K_{st} にて暗号化した値 $E_{nc}(K_{st}, K_{co})$ を光ディスク記録再生装置 100 に送信する。

【0081】

セキュリティモジュール 13 から上記値 $E_{nc}(K_{st}, K_{co})$ を受け取ると、光ディスク記録再生装置 100 は、手順 R18 として、上記暗号鍵 K_{co} を用いて暗号化したコンテンツデータを光ディスク情報記録媒体 10 の光ディスク 12 に記録すると共に、上記暗号鍵 K_{co} をストレージ鍵 K_{st} にて暗号化した値 $E_{nc}(K_{st}, K_{co})$ も上記光ディスク情報記録媒体 10 の光ディスク 12 に記録する。

【0082】

なお、上記リボケーションリストの伝送は、上記コンテンツデータの伝送の間、または終了後に行ってもよい。

【0083】

上記図 7 の例では、セキュリティモジュール 13 と光ディスク記録再生装置 100 において、手順 R12, R13 のように、自己が保持しているリボケーションリスト内にそれぞれ相手方の ID が掲載されているか否かの検証を行った後、手順 R14, R15 にてリボケーションリストのバージョンナンバーの新旧をチェックし、新しいバージョンのリボケーションリストで古いバージョンのリボケーションリストを更新する例を挙げたが、以下に説明するように、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方の ID が掲載されているか否かを検証するようにしてもよい。この場合、必ず新しいバージョンのリボケーションリストによって相手方の ID がチェックされるため、より確実に不正なものであるか否かを判定できる。なお、両者のリボケーションリストのバージョンナンバーが同じ場合もあり得るので、以下の説明では、バージョンナンバーが同じ場合も考慮して説明する。

【0084】

図 8 には、上述したように、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方の ID を検証するようにした場合の、データ記録時の手順を示す。

【0085】

この図8において、光ディスク記録再生装置100は、先ず、手順R21として、前記図7の手順R11と同様に乱数 R_B を生成し、この乱数 R_B を記録コマンドと共にセキュリティモジュール13に送る。

【0086】

上記記録コマンドと乱数 R_B を受け取ったセキュリティモジュール13は、前記図7の手順R12と同様に、手順R22として、乱数 R_A を発生すると共に前記所定値或いは乱数の K_A を生成し、 $V_A = K_A \cdot G$ の計算を行う。また、セキュリティモジュール13は、前記同様にビット列 $R_A || R_B || V_A || \text{Rev}V_A$ にデジタル署名を行い $\text{Sig}_A = \text{Sign}(\text{PriKey}_A, R_A || R_B || V_A || \text{Rev}V_A)$ を生成し、これら $R_A, R_B, V_A, \text{Rev}V_A, \text{Sig}_A$ に証明書 Cert_A を付けて光ディスク記録再生装置100に送る。

【0087】

上記セキュリティモジュール13から $\text{Cert}_A, R_A, R_B, V_A, \text{Rev}V_A, \text{Sig}_A$ を受け取ると、光ディスク記録再生装置100は、セキュリティモジュール13の証明書 Cert_A 、デジタル署名 Sig_A の検証（チェック）を行う。

【0088】

すなわち、光ディスク記録再生装置100は、先ず、セキュリティモジュール13の証明書 Cert_A の検証を行い、例えば当該検証をパスできないときには、そのセキュリティモジュール13を備えた光ディスク情報記録媒体10を不正な媒体とみなして当該プロトコルを終了する。

【0089】

一方、セキュリティモジュール13の証明書 Cert_A の検証において正当であると判定された場合、光ディスク記録再生装置100は、上記証明書 Cert_A からパブリック鍵 PubKey_A を手に入れる。次に、光ディスク記録再生装置100は、セキュリティモジュール13から返送されてきた乱数 R_B と、当該光ディスク記録再生装置100が手順R21で生成した乱数 R_B とが等しく、さらに上記デジタル署名 Sig_A が正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール13を備えた光ディスク情報記録媒体10が不

正な媒体であると判断して当該プロトコルを終了する。

【0090】

上述のように、セキュリティモジュール13から返送されてきた乱数 R_B と先に生成したものが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、光ディスク記録再生装置100は、図7の手順R13と同様に、手順R23として、 K_B ($0 < K_B < r$) を生成し、 $V_B = K_B \cdot G$ の計算を行う。更に、光ディスク記録再生装置100は、上記乱数 R_B 、乱数 R_A 、値 V_B 、リボケーションリストバージョンナンバー $RevV_B$ からなるビット列 $R_B || R_A || V_B || RevV_B$ にデジタル署名を行って $Sig_B = \text{Sign}(\text{PriKey}_B, R_B || R_A || V_B || RevV_B)$ を生成し、これら R_B 、 R_A 、 V_B 、 $RevV_B$ 、 Sig_B に証明書 $Cert_B$ を付けてセキュリティモジュール13に送る。

【0091】

上記光ディスク記録再生装置100から $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RevV_B$ 、 Sig_B を受け取ると、セキュリティモジュール13は、光ディスク記録再生装置100の証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行う。

【0092】

すなわち、セキュリティモジュール13は、先ず、光ディスク記録再生装置100の証明書 $Cert_B$ の検証を行い、例えば当該検証をパスできないときには、その光ディスク記録再生装置100を不正な装置とみなして当該プロトコルを終了する。

【0093】

一方、光ディスク記録再生装置100の証明書 $Cert_B$ の検証において正当であると判定された場合、セキュリティモジュール13は、上記証明書 $Cert_B$ からパブリック鍵 PubKey_B を手に入れる。次に、セキュリティモジュール13は、光ディスク記録再生装置100から返送されてきた乱数 R_A と、当該セキュリティモジュール13が手順R22で生成した乱数 R_A とが等しく、さらに上記デジタル署名 Sig_B が正当であると判定されたときには、次の処理に進み、そうでない場合には光ディスク記録再生装置100が不正な装置であると判断して当該プロトコルを終了する。

【0094】

上述のように、セキュリティモジュール13と光ディスク記録再生装置100の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール13では $K_A \cdot V_B$ の計算を行い、また、光ディスク記録再生装置100では $K_B \cdot V_A$ の計算を行い、さらにそれらのx座標の下位zビットをセッション鍵Kseとしてこれらセキュリティモジュール13と光ディスク記録再生装置100が共有する。

【0095】

また、セキュリティモジュール13と光ディスク記録再生装置100の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール13と光ディスク記録再生装置100は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行う。

【0096】

ここで、両者のバージョンナンバーが同じである場合、光ディスク記録再生装置100とセキュリティモジュール13は、それぞれが保持するリボケーションリストを用いて相手方のIDの検証を行い、互いに相手方のIDがリボケーションリストに掲載されていないことを検証する。すなわち、セキュリティモジュール13では、光ディスク記録再生装置の ID_B が自己のリボケーションリストに掲載されていないことを検証し、光ディスク記録再生装置100では、セキュリティモジュール13の ID_A が自己のリボケーションリストに掲載されていないことを検証する。当該相互検証の結果、両者において共にリボケーションリストに掲載されていないと判定された場合には、後段の手順R26の処理に進む。また、セキュリティモジュール13において、光ディスク記録再生装置100の ID_B が自己のリボケーションリストに掲載されている場合には、当該光ディスク記録再生装置100は不正な装置であると判定し、当該プロトコルを終了する。同じく、光ディスク記録再生装置100において、セキュリティモジュール13の ID_A が自己のリボケーションリストに掲載されている場合には、当該セキュリティモジュール13は不正な媒体のものであると判定し、当該プロトコルを終了する。

【0097】

一方、セキュリティモジュール13と光ディスク記録再生装置100においてそれぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順R24又はR25として、上記新しいバージョンのリボケーションリストを相手方に送る。この新しいバージョンのリボケーションリストを受け取った側では当該新しいバージョンのリボケーションリストを用いて、相手方のIDの検証を行う。すなわち、セキュリティモジュール13と光ディスク記録再生装置100は、それぞれが当該新しいバージョンのリボケーションリストを用いて、互いに相手方のIDの検証を行う。

【0098】

すなわち例えば、セキュリティモジュール13のリボケーションリストのバージョンが、光ディスク記録再生装置100のものよりも新しい場合、セキュリティモジュール13では自己が保持するリボケーションリストを用いて光ディスク記録再生装置100のID_Bの検証を行い、その検証の結果、光ディスク記録再生装置100がリボケーションリストに記載されていないとき、手順R24として、自己が保持しているリボケーションリストを光ディスク記録再生装置100に送る。当該リボケーションリストを受け取った光ディスク記録再生装置100は、この送られてきたリボケーションリストのバージョンナンバーRevV_Aを先に取得しているバージョンナンバーと同じかどうかチェックし、さらに、その新しいリボケーションリストを用いてセキュリティモジュール13のID_Aの検証を行う。その検証の結果、セキュリティモジュール13のID_Aがリボケーションリストに記載されていない場合には、上記セキュリティモジュール13から送られてきた当該新しいバージョンのリボケーションリスト内に含まれるセンタTCの署名TCSigを検証し、この署名TCSigが正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新する。一方、署名TCSigが正しくない場合は、当該プロトコルを終了する。

【0099】

また例えば、光ディスク記録再生装置100のリボケーションリストのバージ

オンが、セキュリティモジュール13のものよりも新しい場合、光ディスク記録再生装置100では自己が保持するリボケーションリストを用いてセキュリティモジュール13のID_Aの検証を行い、その検証の結果、セキュリティモジュール13がリボケーションリストに記載されていないとき、手順R25として、自己が保持しているリボケーションリストをセキュリティモジュール13に送る。当該リボケーションリストを受け取ったセキュリティモジュール13は、この送られてきたリボケーションリストのバージョンナンバーRevV_Bを先に取得しているバージョンナンバーと同じかどうかチェックし、さらに、その新しいリボケーションリストを用いて光ディスク記録再生装置100のID_Bの検証を行い、その検証の結果、光ディスク記録再生装置100のID_Bがリボケーションリストに記載されていないとき、上記光ディスク記録再生装置100から送られてきた新しいバージョンのリボケーションリスト内に含まれるセンタTCの署名TCSigを検証し、当該署名TCSigが正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新する。一方、署名TCSigが正しくない場合は、当該プロトコルを終了する。

【0100】

その後、光ディスク記録再生装置100は、手順R26として、光ディスク12に記録するコンテンツデータを暗号化するための暗号鍵Kcoを定め、この暗号鍵Kcoをセッション鍵Kseにて暗号化した値Enc(Kse, Kco)をセキュリティモジュール13に送信する。

【0101】

セキュリティモジュール13は、手順R27として、上記光ディスク記録再生装置100から送信されてきた値Enc(Kse, Kco)をセッション鍵Kseを用いて復号することにより、暗号鍵Kcoを復元し、さらに、この暗号鍵Kcoを自己が持つストレージ鍵Kstにて暗号化した値Enc(Kst, Kco)を光ディスク記録再生装置100に送信する。

【0102】

セキュリティモジュール13から上記値Enc(Kst, Kco)を受け取ると、光ディスク記録再生装置100は、手順R28として、上記暗号鍵Kcoを用いて暗号

化したコンテンツデータを光ディスク情報記録媒体 10 の光ディスク 12 に記録すると共に、上記暗号鍵 K_{co} をストレージ鍵 K_{st} にて暗号化した値 $E_{nc}(K_{st}, K_{co})$ も上記光ディスク情報記録媒体 10 の光ディスク 12 に記録する。

【0103】

次に、図 9～図 11 を用いて、上記第 1 の実施の形態の光ディスク記録再生装置 100 が光ディスク 12 からデータを再生する手順を説明する。

【0104】

なお、上述したように、第 1 の実施の形態の光ディスク記録再生装置 100 は、センタ TC から与えられた ID、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを上記不揮発性メモリ 110 に格納しており、また同様に、当該第 1 の実施の形態の光ディスク情報記録媒体 10 のセキュリティモジュール 13 は、センタ TC から与えられた ID、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを上記不揮発性メモリ 34 に格納している。また、光ディスク記録再生装置 100 は、再生すべきデータに付与されたレコーディング ID (Recording-ID) を知っているものとする。

【0105】

先ず、図 9 において、光ディスク記録再生装置 100 は、手順 P1 として、光ディスク情報記録媒体 10 のセキュリティモジュール 13 に対して、これからデータの再生を行うことを示す再生コマンド（再生開始コマンド）とレコーディング ID とを送る。

【0106】

次に、手順 P2 として、光ディスク記録再生装置 100 及び光ディスク情報記録媒体 10 のセキュリティモジュール 13 は、上記再生コマンドをトリガーとして、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する。

【0107】

このプロトコルの内容は、データの記録時に用いられるプロトコルと同様であり、それぞれ他方が持つ公開鍵と秘密鍵が正しいことの検証と、リボケーションリストに相手方の ID が載せられていないことの確認を互に行い、セッション鍵 K_{se} を共有し、また自分が持つリボケーションリストのバージョンナンバーを

送り合う。また、手順 P 3, P 4 として、どちらかが相対的に新しいリボケーションリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のリボケーションリストを更新することも同様である。

【0108】

次に、データを光ディスク 12 から読み出す前に、このデータを暗号化したときの暗号鍵 Kco を光ディスク記録再生装置 100 が知ることが必要になる。

【0109】

暗号鍵 Kco は、セキュリティモジュール 13 が安全にその内部の不揮発性メモリ 34 に格納しているか、或いはセキュリティモジュール 13 が予め格納しているストレージ鍵 Kst を用いて当該暗号鍵 Kco を暗号化した値 Enc (Kst, Kco) として光ディスク 12 に記録されている。なお、ここでは、不揮発性メモリ 34 に暗号鍵 Kco が安全に格納されているとする。

【0110】

前者の場合、セキュリティモジュール 13 は、手順 P 5 として、不揮発性メモリ 34 に格納されている暗号鍵 Kco をセッション鍵 Kse で暗号化した値 Enc (Kse, Kco) を、光ディスク記録再生装置 100 に送る。光ディスク記録再生装置 100 では、当該値 Enc (Kse, Kco) をセッション鍵 Kse を用いて復号することにより暗号鍵 Kco を得る。

【0111】

一方、後者の場合、光ディスク記録再生装置 100 は、先ず、光ディスク 12 から上記暗号鍵 Kco を暗号化した値 Enc (Kst, Kco) を読み出し、これをセキュリティモジュール 13 に送る。セキュリティモジュール 13 は、ストレージ鍵 Kst を用いてこれを復号して暗号鍵 Kco を得、これをセッション鍵 Kse で暗号化した値 Enc (Kse, Kco) を、手順 P 5 として光ディスク記録再生装置 100 に送る。光ディスク記録再生装置 100 は、当該値 Enc (Kse, Kco) をセッション鍵 Kse を用いて復号することにより暗号鍵 Kco を得る。

【0112】

上述のように、光ディスク記録再生装置 100 は、手順 P 5 により、データを暗号化したときの暗号鍵 Kco を得ることができる。

【0113】

次に、手順P6として、光ディスク記録再生装置100は、光ディスク12から、上記暗号鍵 K_{co} を用いて暗号化されているデータ $E_{nc}(K_{co}, data)$ を読み出し、先に取得した暗号鍵 K_{co} を用いてこれを復号し使用する。

【0114】

以上が、光ディスク12からデータを読み出す処理の基本的な手順である。

【0115】

図10には、上記図7に示した第1の実施の形態の光ディスク記録再生装置100が光ディスク情報記録媒体10の光ディスク12から、上記暗号化されているデータを読み出すまでの手順の詳細を説明する。なお、この図10では、前述の図7等と同様に、光ディスク記録再生装置100に係る各情報について「B」の文字を付し、セキュリティモジュール13に係る各情報について「A」の文字を付している。また、図9で説明したのと同様に、光ディスク記録再生装置100とセキュリティモジュール13は、センタTCから与えられたID（セキュリティモジュール13の ID_A 、光ディスク記録再生装置100の ID_B ）、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを、それぞれ対応する不揮発性メモリ110、34に格納している。

【0116】

図10において、先ず、光ディスク記録再生装置100は、手順P11として、前記前記記録時と同様に、乱数発生部107にて64ビットの乱数 R_B を生成し、この乱数 R_B を再生コマンド（再生開始コマンド）と共にセキュリティモジュール13に送る。

【0117】

上記再生コマンドと乱数 R_B を受け取ったセキュリティモジュール13は、手順P12として、前記記録時と同様に、乱数発生部33にて64ビットの乱数 R_A を発生すると共に、前記同様の秘密の所定値或いは乱数の K_A ($0 < K_A < r$) を生成し、前記EC-DHアルゴリズムの第1段階（ステップ1）において $V_A = K_A \cdot G$ の計算を行い、更に、前記EC-DSAの署名アルゴリズムを用いて、上記乱数 R_A 、乱数 R_B 、値 V_A 、リボケーションリストのバージョンナンバー

RevV_Aからなるビット列 $R_A || R_B || V_A || \text{Rev}V_A$ にデジタル署名を行った $\text{Sig}_A = \text{Sign}(\text{PriKey}_A, R_A || R_B || V_A || \text{Rev}V_A)$ を得る。セキュリティモジュール13は、これら $R_A, R_B, V_A, \text{Rev}V_A, \text{Sig}_A$ に証明書 Cert_A を付け、光ディスク記録再生装置100に送る。

【0118】

上記セキュリティモジュール13から $\text{Cert}_A, R_A, R_B, V_A, \text{Rev}V_A, \text{Sig}_A$ を受け取ると、光ディスク記録再生装置100は、前述の記録時と同様に、E-CDSAの証明アルゴリズムを用いて、セキュリティモジュール13の証明書 Cert_A 、デジタル署名 Sig_A 、 ID_A の検証（チェック）を行う。すなわち、光ディスク記録再生装置100は、セキュリティモジュール13の証明書 Cert_A の検証を行い、当該検証をパスできないときには、そのセキュリティモジュール13を備えた光ディスク情報記録媒体10を不正な媒体とみなして当該プロトコルを終了し、一方、当該検証において正当であると判定された場合には、上記証明書 Cert_A からパブリック鍵 PubKey_A を手に入れる。

【0119】

次に、光ディスク記録再生装置100は、セキュリティモジュール13から返送されてきた乱数 R_B と上記手順P11で生成した乱数 R_B とが等しく、且つデジタル署名 Sig_A が正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール13を備えた光ディスク情報記録媒体10が不正な媒体であると判断して当該プロトコルを終了する。

【0120】

上記セキュリティモジュール13から返送されてきた乱数 R_B と先に生成したものが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、前述の記録時と同様に、光ディスク記録再生装置100は、自己が保持しているリボケーションリストを用い、セキュリティモジュール13の ID_A が当該リボケーションリストに掲載されていないことを検証し、その検証の結果、上記 ID_A がリボケーションリストに掲載されている場合には、当該セキュリティモジュール13を備えた光ディスク情報記録媒体10は不正な媒体であると判定し、当該プロトコルを終了する。一方、上記 ID_A が当該リボケーションリストに掲載されて

おらず正当な媒体であると判断した場合、光ディスク記録再生装置 100 は、手順 P 13 として、前記記録時と同様に、所定値或いは乱数の K_B ($0 < K_B < r$) を生成し、前記 EC-DH アルゴリズムの第 1 段階 (ステップ 1) において $V_B = K_B \cdot G$ の計算を行い、更に、前記 EC-DSA の署名アルゴリズムを用いて、乱数 R_B 、乱数 R_A 、値 V_B 、バージョンナンバー $\text{Rev}V_B$ からなるビット列 $R_B || R_A || V_B || \text{Rev}V_B$ にデジタル署名を行って $\text{Sig}_B = \text{Sign}(\text{PriKey}_B, R_B || R_A || V_B || \text{Rev}V_B)$ を得る。光ディスク記録再生装置 100 は、これら R_B 、 R_A 、 V_B 、 $\text{Rev}V_B$ 、 Sig_B に証明書 Cert_B を付け、セキュリティモジュール 13 に送る。

【0121】

上記光ディスク記録再生装置 100 から Cert_B 、 R_B 、 R_A 、 V_B 、 $\text{Rev}V_B$ 、 Sig_B を受け取ると、セキュリティモジュール 13 は、EC-DSA の証明アルゴリズムを用いて、光ディスク記録再生装置 100 の証明書 Cert_B 、デジタル署名 Sig_B 、 ID_B の検証 (チェック) を行う。すなわち、セキュリティモジュール 13 は、先ず証明書 Cert_B の検証を行い、例えば当該検証をパスできないときには、その光ディスク記録再生装置 100 を不正な装置とみなして当該プロトコルを終了し、一方、上記証明書 Cert_B の検証において正当であると判定された場合、上記証明書 Cert_B からパブリック鍵 PubKey_B を手に入れる。次に、セキュリティモジュール 13 は、光ディスク記録再生装置 100 から返送されてきた乱数 R_A と、先に手順 P 12 で生成した乱数 R_A とが等しく、且つデジタル署名 Sig_B が正当であると判定されたときには、次の処理に進み、そうでない場合には光ディスク記録再生装置 100 が不正な装置であると判断して当該プロトコルを終了する。

【0122】

上述のように、光ディスク記録再生装置 100 から返送されてきた乱数 R_A と先に生成したものとは等しく、且つデジタル署名 Sig_B が正当であると判定されたとき、セキュリティモジュール 13 は、自己が保持するリボケーションリストに光ディスク記録再生装置 100 の ID_B が記載されていないことを検証し、その検証の結果、光ディスク記録再生装置 100 の ID_B がリボケーションリストに掲載されている場合には、当該光ディスク記録再生装置 100 は不正な装置で

あると判定し、当該プロトコルを終了する。

【 0 1 2 3 】

光ディスク記録再生装置 100 の ID_B が当該リボケーションリストに掲載されておらず、その光ディスク記録再生装置 100 が正当であると判断した場合、すなわちセキュリティモジュール 13 と光ディスク記録再生装置 100 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 13 では $K_A \cdot V_B$ の計算を行い、また、光ディスク記録再生装置 100 では $K_B \cdot V_A$ の計算を行い、さらにそれらの x 座標の下位 z ビットをセッション鍵 K_{se} としてこれらセキュリティモジュール 13 と光ディスク記録再生装置 100 が共有する。

~~【0124】~~

次に、前記記録時と同様に、セキュリティモジュール 13 と光ディスク記録再生装置 100 は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順 P14 又は P15 として、その新しいバージョンのリボケーションリストを相手方に送る。このように、相手方から新しいバージョンナンバーのリボケーションリストが送られてきた方は、当該リボケーションリスト内に含まれるセンタ TC の署名 TC Sig を検証し、当該署名 TC Sig が正しい場合にのみ、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新（リストのアップデート）する。

【0 1 2 5】

次に、光ディスク記録再生装置 100 は、暗号化されているデータを光ディスク 12 から読み出す前に、このデータを暗号化したときの暗号鍵 K_{co} を取得し、当該取得した暗号鍵 K_{co} を用いて、上記光ディスク 12 から読み出した暗号化されているデータを復号する。なお、図 10 の例では、セキュリティモジュール 13 がストレージ鍵 K_{st} を用いて暗号化した値 $E_{nc}(K_{st}, K_{co})$ が光ディスク 12 に記録されているとする。この場合、光ディスク記録再生装置 100 は、先ず、手順 P16 として、光ディスク 12 から上記ストレージ鍵 K_{st} で暗号鍵 K_{co} を暗号化した値 $E_{nc}(K_{st}, K_{co})$ を読み出し、次に手順 P17 として、当該値 $E_{nc}($

Kst, Kco) をセキュリティモジュール 13 に送る。セキュリティモジュール 13 では、予め保持しているストレージ鍵 Kst を用いてこれを復号して暗号鍵 Kco を得、当該暗号鍵 Kco をセッション鍵 Kse で暗号化し、その値 Enc (Kse, Kco) を手順 P18 として光ディスク記録再生装置 100 に送る。光ディスク記録再生装置 100 は、当該値 Enc (Kse, Kco) をセッション鍵 Kse を用いて復号することで、暗号鍵 Kco を得る。

【0126】

その後、光ディスク記録再生装置 100 は、手順 P19 により、暗号鍵 Kco にて暗号化されているデータ Enc (Kco, data) を光ディスク 12 から読み出し、これを先に取得した暗号鍵 Kco を用いて復号する。

【0127】

上記図 10 の例では、セキュリティモジュール 13 と光ディスク記録再生装置 100 において、手順 P12, P13 のように、自己が保持しているリボケーションリスト内にそれぞれ相手方の ID が掲載されているか否かの検証を行った後、手順 P14, P15 にてリボケーションリストのバージョンナンバーの新旧をチェックし、新しいバージョンのリボケーションリストで古いバージョンのリボケーションリストを更新する例を挙げたが、当該再生の場合も前述した記録の場合と同様に、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方の ID が掲載されているか否かを検証するようにしてもよい。この場合、必ず新しいバージョンのリボケーションリストによって相手方の ID がチェックされるため、より確実に不正なものであるか否かを判定できる。なお、この再生の例の場合も、前述の図 8 の例と同様に、両者のリボケーションリストのバージョンナンバーが同じ場合もあり得るので、以下の説明では、バージョンナンバーが同じ場合も考慮して説明する。

【0128】

図 11 には、光ディスク 12 からのデータ再生時において、上述したように、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方の ID を検証するようにし

た場合の手順を示す。

【0129】

この図11において、光ディスク記録再生装置100は、先ず、手順P21として、前記図10の手順P11と同様に乱数 R_B を生成し、この乱数 R_B を再生コマンドと共にセキュリティモジュール13に送る。

【0130】

上記再生コマンドと乱数 R_B を受け取ったセキュリティモジュール13は、前記図10の手順P12と同様に、手順P22として、乱数 R_A と前記所定値或いは乱数の K_A を生成し、 $V_A = K_A \cdot G$ の計算を行い、更に前記同様にビット列 $R_A || R_B || V_A || \text{Rev}V_A$ にデジタル署名を行って $\text{Sig}_A = \text{Sign}(\text{PriKey}_A, R_A || R_B || V_A || \text{Rev}V_A)$ を生成し、これらに証明書 Cert_A を付けて光ディスク記録再生装置100に送る。

【0131】

上記セキュリティモジュール13から Cert_A 、 R_A 、 R_B 、 V_A 、 $\text{Rev}V_A$ 、 Sig_A を受け取ると、光ディスク記録再生装置100は、セキュリティモジュール13の証明書 Cert_A とデジタル署名 Sig_A の検証を行う。すなわち、光ディスク記録再生装置100は、上記証明書 Cert_A の検証を行い、当該証明書 Cert_A の検証において正当であると判定された場合に、上記証明書 Cert_A からパブリック鍵 PubKey_A を手に入れ、次に、セキュリティモジュール13から返送されてきた乱数 R_B と手順P21で生成した乱数 R_B とが等しく、且つデジタル署名 Sig_A が正当であると判定されたときのみ次の処理に進む。

【0132】

上述のように正当であると判定されたとき、光ディスク記録再生装置100は、図10の手順P13と同様に、手順P23として、 K_B ($0 < K_B < r$) を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、乱数 R_B 、乱数 R_A 、値 V_B 、バージョンナンバー $\text{Rev}V_B$ からなるビット列 $R_B || R_A || V_B || \text{Rev}V_B$ にデジタル署名を行って $\text{Sig}_B = \text{Sign}(\text{PriKey}_B, R_B || R_A || V_B || \text{Rev}V_B)$ を生成し、これら R_B 、 R_A 、 V_B 、 $\text{Rev}V_B$ 、 Sig_B に証明書 Cert_B を付けてセキュリティモジュール13に送る。

【0 1 3 3】

上記光ディスク記録再生装置 1 0 0 から $Cert_B$, R_B , R_A , V_B , $RevV_B$, Sig_B を受け取ると、セキュリティモジュール 1 3 は、光ディスク記録再生装置 1 0 0 の証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行う。セキュリティモジュール 1 3 は、上記証明書 $Cert_B$ の検証の結果、正当であると判定された場合、上記証明書 $Cert_B$ からパブリック鍵 $PubKey_B$ を手に入れ、次に、光ディスク記録再生装置 1 0 0 から返送されてきた乱数 R_A と前記手順 P 2 2 で生成した乱数 R_A とが等しく、且つデジタル署名 Sig_B が正当であると判定されたとき、次の処理に進む。

【0 1 3 4】

上述のように、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 1 3 では $K_A \cdot V_B$ の計算を行い、光ディスク記録再生装置 1 0 0 では $K_B \cdot V_A$ の計算を行い、さらにそれらの x 座標の下位 z ビットをセッション鍵 K_{se} としてこれらセキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 が共有する。また、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行う。

【0 1 3 5】

ここで、両者のバージョンナンバーが同じである場合、光ディスク記録再生装置 1 0 0 とセキュリティモジュール 1 3 は、それぞれが保持するリボケーションリストを用いて相手方の ID の検証を行い、互いに相手方の ID がリボケーションリストに掲載されていないことを検証する。

【0 1 3 6】

一方、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 においてそれぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順 P 2 4 又は P 2 5 として、上記新しいバージョンのリボケ

ーションリストを相手方に送り、この新しいバージョンのリボケーションリストを受け取った側では当該新しいバージョンのリボケーションリストを用いた相手方のID検証を行うと共に、古いバージョンのリボケーションリストを更新する。

【0137】

その後、光ディスク記録再生装置100は、手順P26として、光ディスク12から上記ストレージ鍵Kstで暗号鍵Kcoを暗号化した値Enc(Kst, Kco)を読み出し、次に手順P27として、当該値Enc(Kst, Kco)をセキュリティモジュール13に送る。セキュリティモジュール13において、ストレージ鍵Kstにより復号され、更にセッション鍵Kseで暗号鍵Kcoを暗号化した値Enc(Kse, Kco)は、~~手順P28として光ディスク記録再生装置100に送られ、光ディスク記録再生装置100では、当該値Enc(Kse, Kco)をセッション鍵Kseを用いて復号することで、暗号鍵Kcoを得る。~~その後、光ディスク記録再生装置100は、手順P29により、光ディスクから、データEnc(Kco, data)を読み出し、先に取得した暗号鍵Kcoを用いて、その復号を行う。

【0138】

次に、本発明の第2の実施の形態について説明する。

【0139】

本発明の第2の実施の形態では、情報記録媒体として、メモリ情報記録媒体を用いる。

【0140】

図12には、本実施の形態のメモリ情報記録媒体20の構成例を示す。

【0141】

このメモリ情報記録媒体20は、カートリッジ21内に、データを記録するための電氣的に消去可能な大容量不揮発性メモリ（具体的には例えばフラッシュROMやEEPROM、磁気抵抗効果を用いたMRAM (Magnetic Random Access Memory) など）からなるメモリ部22と、セキュリティモジュール23を備えている。

【0 1 4 2】

上記セキュリティモジュール 2 3 は、図 1 3 に示すように、主要構成要素として、外部インターフェース部 4 1、演算部 4 2、乱数発生部 4 3、不揮発性メモリ 4 4、制御部 4 5、記録媒体インターフェース部 4 6 を備えている。

【0 1 4 3】

すなわち、このセキュリティモジュール 2 3 は、図 2 に示したセキュリティモジュール 1 3 と略々同じ構成及び機能を有するが、当該セキュリティモジュール 2 3 の場合、外部とのインターフェース手段として外部インターフェース部 4 1 を備えている。また、このセキュリティモジュール 2 3 は、カートリッジ 2 1 内のメモリ部 2 2 との間のインターフェースをとるための記録媒体インターフェース（例えばフラッシュ ROM インターフェースなど）4 6 を備えており、したがって、前記メモリ部 2 2 への情報の記録（書き込み）、再生（読み出し）は、当該セキュリティモジュール 2 3 を介して行われる。

【0 1 4 4】

このセキュリティモジュール 2 3 内部の不揮発性メモリ 4 4 は、秘密性の必要な情報や耐改ざん性が必要な情報など、重要な情報を格納するのに用いられるが、もしこのメモリ 4 4 の容量が十分でない場合には、セキュリティモジュール 2 3 外の、一般データを記録するための大容量のメモリ部 2 2 にこれらの重要な情報を記録することもできる。この場合、秘密性の必要な情報については、セキュリティモジュール 2 3 内の不揮発性メモリ 4 4 に安全に格納してあるストレージ鍵 K_{st} により暗号化する方法を用いて保護し、耐改ざん性が必要な情報については、重要な情報を記録するメモリ部 2 2 のブロックのいわゆる ICV (Integrity Check Value) を計算し、セキュリティモジュール 2 3 内の不揮発性メモリ 4 4 に格納しておき、セキュリティモジュール 2 3 外のメモリ部 2 2 から情報を読み出す際に再びそのブロックの ICV を計算し、格納してある値と比較することによって情報が改ざんされていないことを確認するなどの保護策をとる。

【0 1 4 5】

ICV は、あるデータの完全性 (Integrity、改ざんされていないこと) を保証するために、データと、何らかの秘密値（この場合、例えばセキュリティモジ

ジュール 23 のストレージ鍵 K_{st}) とを入力とし、予め定められたアルゴリズムによって計算される値である。これによれば、上記の秘密値を知っているものしか任意のデータに対する ICV を計算することが事実上できないため、例えばデータが変更されたような場合には、読み出し時に同様の方法で計算される ICV と記録時に計算されてセキュリティモジュール 23 内に格納されている値とが異なることになるため、上記データが変更された事実をセキュリティモジュール 23 は知ることができるようになる。

【0146】

なお、ICV を計算するアルゴリズムとしては、公開鍵暗号技術を用いたデジタル署名アルゴリズムや、共通鍵暗号技術を用いた MAC (Message Authentication Code) 作成アルゴリズム、鍵つきハッシュ関数を用いるアルゴリズムなどがある。ICV については、例えば、Menezes の他、「Handbook of applied cryptography」、CRC、ISBN 0-8493-8523-7、pp. 352-368 に詳しい解説がある。

【0147】

図 14 は、上記第 2 の実施の形態のメモリ情報記録媒体 20 に対してデータ等の記録／再生（書き込み／読み出し）を行うメモリ記録再生装置 200 の構成例を表している。

【0148】

この図 14 に示したメモリ記録再生装置 200 は、主要構成要素として、入出力端子 201、制御部 205、入力部 206、乱数発生部 207、インターフェース部 208、演算部 209、不揮発性メモリ 210 などを備えて成る。

【0149】

このメモリ記録再生装置 200 は、図 3 に示した光ディスク記録再生装置 100 とその構成が略々同じであるが、図 3 における光ディスク 12 用の構成要素であるスピンドルモータ 101、光学ヘッド 102 やサーボ回路 103 などは存在せず、その代わりに、セキュリティモジュール 23 を介してメモリ情報記録媒体 20 への記録／再生のためのインターフェースが設けられる。なお、図 14 の例では、セキュリティモジュール 23 にアクセスするためのインターフェース部 208 が、上記メモリ情報記録媒体 20 への記録／再生のためのインターフェース

の機能を兼用している。また、この図 14 の場合、メモリ情報記録媒体 20 の入出力端子 24 と、メモリ記録再生装置 200 の入出力端子 201 が電氣的に接続される。

【0150】

記録／再生回路 204 は、制御部 205 により動作モードが切り換えられる暗号化部 204 A と復号部 204 B を有する。暗号化部 204 A は、記録モード時に、外部から記録信号の供給を受けると、その記録信号を暗号化し、インターフェース部 208 に供給して、メモリ情報記録媒体 20 のメモリ部 22 に記録させる。復号部 204 B は、再生モード時に、メモリ情報記録媒体 20 のメモリ部 22 から再生されたデータを復号し、外部に再生信号として出力する。

【0151】

また、入力部 206 は、前記図 3 の入力部 106 と同様に、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作がなされたとき、その入力操作に対応する信号を出力する。制御部 205 は、記憶されている所定のコンピュータプログラムに従って、装置全体を制御する。乱数発生部 207 は、制御部 205 の制御により、所定の乱数を発生する。インターフェース 208 部は、メモリ情報記録媒体 20 の入出力端子 24 及びメモリ記録再生装置 200 の入出力端子 201 を介して、メモリ情報記録媒体 20 のセキュリティモジュール 23 との間でデータの授受を行う。

【0152】

さらに、この第 2 の実施の形態のメモリ記録再生装置 200 は、演算部 209 と不揮発性メモリ 210 をも備えている。これら演算部 209 及び不揮発性メモリ 210 は、前記図 3 の構成の演算部 109 及び不揮発性メモリ 110 と同様の機能を有している。

【0153】

次に、図 15 から図 18 を用いて、第 2 の実施の形態のメモリ記録再生装置 200 がメモリ情報記録媒体 20 にデータを記録する手順を説明する。

【0154】

なお、当該第 2 の実施の形態のメモリ記録再生装置 200 は、センタ TC から

与えられた ID、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを上記不揮発性メモリ 2 1 0 に格納しており、また同様に、当該第 2 の実施の形態のメモリ情報記録媒体 2 0 のセキュリティモジュール 2 3 は、センタ TC から与えられた ID、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを上記不揮発性メモリ 4 4 に格納している。

【0 1 5 5】

先ず、図 1 5 において、メモリ記録再生装置 2 0 0 は、手順 R 3 1 として、メモリ情報記録媒体 2 0 のセキュリティモジュール 2 3 に対して、これからデータの記録を行うことを示す記録コマンド（記録開始コマンド）と、1 回 1 回の記録を識別するために個別に割り当てるレコーディング ID（Recording-ID）とを送る。

【0 1 5 6】

次に、手順 R 3 2 として、メモリ記録再生装置 2 0 0 及びメモリ情報記録媒体 2 0 のセキュリティモジュール 2 3 は、上記記録コマンドをトリガーとして、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する。このプロトコルの内容は、前述した第 1 の実施の形態におけるデータの記録時に用いられるプロトコルと同様であり、それぞれ他方が持つ公開鍵と秘密鍵が正しいことの検証と、リボケーションリストに相手方の ID が載せられていないことの確認を互に行い、セッション鍵 K_{se} を共有し、また自分が持つリボケーションリストのバージョンナンバーを送り合う。

【0 1 5 7】

また、前記図 6 の手順 R 3, R 4 と同様に、図 1 5 の手順 P 3 3, P 3 4 として、どちらかが相対的に新しいリボケーションリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のリボケーションリストを更新することも同様である。すなわち、手順 R 3 3 には、セキュリティモジュール 2 3 上のリボケーションリストのバージョンが、記録再生装置 2 0 0 上のリボケーションリストのバージョンよりも新しい場合におけるリボケーションリストの流れを示しており、また、手順 R 3 4 には、記録再生装置 2 0 0 上のリボケーションリストのバージョンが、セキュリティモジュール 2 3 上のリボケーションリス

トのバージョンよりも新しい場合におけるリボケーションリストの流れを示している。

【0158】

なお、手順R33、R34におけるリボケーションリストの送付は、後の手順R35、R36におけるデータの記録と順序が前後してもかまわない。つまり、手順R35、R36にてデータの記録を行った後に、手順R33或いはR34でのリボケーションリストの送付を行うようにしてもよい。

【0159】

ここで、当該第2の実施の形態においても前記第1の実施の形態の場合と同様に、データを暗号化する暗号鍵Kcoを決定するが、その決定方法としては、以下に述べる暗号鍵決定方法(11)～(14)のうちの一つを用いればよい。

【0160】

すなわち、この第2の実施の形態の場合、暗号鍵決定方法(11)では、 $Kse = Kco$ とする。この時、セキュリティモジュール23は、暗号鍵Kcoを安全にその内部の不揮発性メモリ44に格納するか、セキュリティモジュール23が予め格納しているストレージ鍵Kstを用いて当該暗号鍵Kcoを暗号化した値 $Enc(Kst, Kco)$ を、当該セキュリティモジュール23外のメモリ部22に格納する。

【0161】

暗号鍵決定方法(12)では、セキュリティモジュール23が予め格納しているストレージ鍵Kstを暗号鍵Kcoとする。この場合、セキュリティモジュール23がストレージ鍵Kstを上記セッション鍵Kseで暗号化してメモリ記録再生装置200に送る。

【0162】

暗号鍵決定方法(13)では、セキュリティモジュール23がそのデータ用の暗号鍵Kcoを乱数発生器などを用いて新たに発生させる。この場合、セキュリティモジュール23が当該暗号鍵Kcoを上記セッション鍵Kseで暗号化してメモリ記録再生装置200に送る。また、セキュリティモジュール23は、暗号鍵Kcoを安全にその内部の不揮発性メモリ44に格納するか、セキュリティモジュール23が予め格納しているストレージ鍵Kstを用いて上記暗号鍵Kcoを暗号化した

値 $E_{nc}(K_{st}, K_{co})$ を上記メモリ部 2 2 に格納する。

【0 1 6 3】

暗号鍵決定方法 (1 4) では、メモリ記録再生装置 2 0 0 がそのデータ用の暗号鍵 K_{co} を乱数発生器などを用いて新たに発生させる。この場合、メモリ記録再生装置 2 0 0 が暗号鍵 K_{co} をセッション鍵 K_{se} で暗号化してセキュリティモジュール 2 3 に送る。セキュリティモジュール 2 3 は暗号鍵 K_{co} を安全にその内部の不揮発性メモリ 4 4 に格納するか、セキュリティモジュール 2 3 が予め格納しているストレージ鍵 K_{st} を用いて暗号鍵 K_{co} を暗号化した値 $E_{nc}(K_{st}, K_{co})$ を上記メモリ部 2 2 に格納する。

【0 1 6 4】

上述した暗号鍵決定方法 (1 1) ~ (1 4) の何れかを用いて暗号鍵 K_{co} を決定したならば、次に、手順 R 3 5 として、メモリ記録再生装置 2 0 0 は、メモリ情報記録媒体 2 0 のメモリ部 2 2 に記録するデータを当該暗号鍵 K_{co} で暗号化し、その暗号化されたデータ $E_{nc}(K_{co}, data)$ をセキュリティモジュール 2 3 に伝送する。

【0 1 6 5】

この時のセキュリティモジュール 2 3 は、手順 R 3 6 として、当該暗号化されたデータ $E_{nc}(K_{co}, data)$ を、上記大容量のメモリ部 2 2 に格納する。

【0 1 6 6】

また、上記暗号化 K_{co} 、又は暗号化した暗号鍵 K_{co} を、セキュリティモジュール 2 3 の不揮発性メモリ 4 4、又はメモリ部 2 2 に記録する際には、レコーディング ID を検索用のキーとするために一緒に記録したり、データが記録されるメモリ部 2 2 のセクタと同一のセクタに、上記暗号化した暗号鍵 K_{co} を記録するなどして、データと暗号鍵 K_{co} との対応がとれるようにしておく。なお、この暗号鍵 K_{co} の管理、伝送と、データの暗号化には、その処理速度の観点から共通鍵暗号アルゴリズムを使用することが好適である。

【0 1 6 7】

また特に、上記暗号鍵決定方法 (1 4) の場合には、メモリ記録再生装置 2 0 0 が暗号鍵 K_{co} を決められるため、メモリ記録再生装置 2 0 0 は予めデータを暗

号化しておくことが可能になる。

【0168】

当該第2の実施の形態では、以上の手順により、データをメモリ情報記録媒体20の大容量メモリ部22に記録する。

【0169】

次に、図16には、上記図15に示した第2の実施の形態のメモリ記録再生装置200がメモリ情報記録媒体20にデータを記録するまでの手順の詳細を示す。なお、この図16では、メモリ記録再生装置200に係る各情報について「B」の文字を付し、メモリ情報記録媒体20のセキュリティモジュール23に係る各情報について「A」の文字を付している。また、図15で説明したのと同様に、メモリ記録再生装置200とセキュリティモジュール23は、センタTCから与えられたID（セキュリティモジュール23のID_A、メモリ記録再生装置200のID_B）、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを、それぞれ対応する不揮発性メモリ210、44に格納している。

【0170】

図16の手順R41～手順R46までは、前述した第1の実施の形態における図7の手順R11～手順R16までと略々同じである。

【0171】

すなわち、メモリ記録再生装置200は、手順R41として乱数R_Bを生成して記録コマンドと共にセキュリティモジュール23に送り、当該記録コマンドと乱数R_Bを受け取ったセキュリティモジュール23は、手順R42として、乱数R_AとK_Aを生成し、次に $V_A = K_A \cdot G$ の計算を行い、乱数R_A、乱数R_B、値V_A、バージョンナンバーRevV_Aからなるビット列にデジタル署名を行ってSig_Aを得、これらR_A、R_B、V_A、RevV_A、Sig_Aと証明書Cert_Aをメモリ記録再生装置200に送る。なお、セキュリティモジュール23がリボケーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして0を用いる。

【0172】

上記セキュリティモジュール23から $Cert_A$, R_A , R_B , V_A , $RevV_A$, Sig_A を受け取ると、メモリ記録再生装置200は、証明書 $Cert_A$ の検証を行い、その検証をパスできないときには、そのセキュリティモジュール23を備えたメモリ情報記録媒体20を不正な媒体とみなして当該プロトコルを終了し、一方、証明書 $Cert_A$ の検証において正当であると判定された場合、上記証明書 $Cert_A$ からパブリック鍵 $PubKey_A$ を手に入れる。次に、メモリ記録再生装置200は、セキュリティモジュール23から返送されてきた乱数 R_B と、先の手順R41で生成した乱数 R_B とが等しく、且つデジタル署名 Sig_A が正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール23を備えたメモリ情報記録媒体20が不正な媒体であると判断して当該プロトコルを終了する。

【0173】

上記セキュリティモジュール23から返送されてきた乱数 R_B と先に生成したものとが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、メモリ記録再生装置200は、自己の不揮発性メモリ210に格納しているリボケーションリストを用い、セキュリティモジュール23を備えたメモリ情報記録媒体20の ID_A が当該リボケーションリストに掲載されていないことを検証し、この検証の結果、上記 ID_A がリボケーションリストに掲載されている場合には、当該セキュリティモジュール23を備えたメモリ情報記録媒体20は不正な媒体であると判定し、当該プロトコルを終了する。一方、上記 ID_A が当該リボケーションリストに掲載されていない場合、メモリ記録再生装置200は、手順R43として、 K_B を生成して $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、バージョンナンバー $RevV_B$ からなるビット列にデジタル署名を行って Sig_B を得る。次にメモリ記録再生装置200は、これら R_B , R_A , V_B , $RevV_B$, Sig_B と証明書 $Cert_B$ を、セキュリティモジュール23に送る。なお、メモリ記録再生装置200がリボケーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして0を用いる。

【0174】

上記メモリ記録再生装置200から $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RevV_B$ 、 Sig_B を受け取ると、セキュリティモジュール23は、上記証明書 $Cert_B$ の検証を行い、当該検証をパスできないときには、そのメモリ記録再生装置200を不正な装置とみなして当該プロトコルを終了し、一方、上記証明書 $Cert_B$ の検証において正当であると判定された場合は、上記証明書 $Cert_B$ からパブリック鍵 $PubKey_B$ を手に入れる。次に、セキュリティモジュール23は、メモリ記録再生装置200から返送されてきた乱数 R_A と先に手順R42で生成した乱数 R_A とが等しく、且つデジタル署名 Sig_B が正当であると判定されたときには、次の処理に進み、そうでない場合にはメモリ記録再生装置200が不正な装置であると判断して当該プロトコルを終了する。

【0175】

上記メモリ記録再生装置200から返送されてきた乱数 R_A と先に生成したものが等しく、且つデジタル署名 Sig_B が正当であると判定されたとき、セキュリティモジュール23は、自己の不揮発性メモリ44に格納しているリボケーションリストを用い、上記 ID_B が当該リボケーションリストに掲載されていないことを検証し、その検証の結果、上記 ID_B がリボケーションリストに掲載されている場合には、当該メモリ記録再生装置200は不正な装置であると判定し、当該プロトコルを終了する。

【0176】

一方、上記 ID_B がリボケーションリストに掲載されていない場合、すなわち、セキュリティモジュール23とメモリ記録再生装置200の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール23では $K_A \cdot V_B$ の計算を行い、また、メモリ記録再生装置200では $K_B \cdot V_A$ の計算を行い、さらにそれらのx座標の下位zビットをセッション鍵 K_{se} としてこれらセキュリティモジュール23とメモリ記録再生装置200が共有する。

【0177】

次に、セキュリティモジュール23とメモリ記録再生装置200は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行

い、自己の保持しているバージョンよりも新しい場合、手順 R 4 4 又は R 4 5 として、その新しいバージョンのリボケーションリストを相手方に送る。このように、相手方から新しいバージョンナンバーのリボケーションリストが送られてきた方は、当該リボケーションリスト内に含まれるセンタ TC の署名 TC Sig を検証し、当該署名 TC Sig が正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新し、一方で、署名 TC Sig が正しくない場合は、当該プロトコルを終了する。

【 0 1 7 8 】

その後、メモリ記録再生装置 2 0 0 は、手順 R 4 6 として、メモリ情報記録媒体 2 0 のメモリ部 2 2 に記録するコンテンツデータを暗号化するための暗号鍵 K co を定め、この暗号鍵 K co をセッション鍵 K se にて暗号化した値 Enc (K se, K co) をセキュリティモジュール 2 3 に送信する。

【 0 1 7 9 】

この時のセキュリティモジュール 2 3 は、手順 R 4 7 として、上記メモリ記録再生装置 2 0 0 から送信されてきた値 Enc (K se, K co) をセッション鍵 K se を用いて復号して暗号鍵 K co を復元し、さらに、この暗号鍵 K co を自己のストレージ鍵 K st にて暗号化した値 Enc (K st, K co) をメモリ部 2 2 に格納し、或いは暗号鍵 K co を不揮発性メモリ 4 4 に格納する。

【 0 1 8 0 】

その後、メモリ記録再生装置 2 0 0 は、手順 R 4 8 として、上記暗号鍵 K co を用いて暗号化したコンテンツデータ Enc (K co, data) をセキュリティモジュール 2 3 に送る。

【 0 1 8 1 】

この時のセキュリティモジュール 2 3 は、手順 R 4 9 として、当該暗号化されているコンテンツデータ Enc (K co, data) をメモリ部 2 2 に格納する。

【 0 1 8 2 】

なお、上記リボケーションリストの伝送は、上記コンテンツデータの伝送の間、または終了後に行ってもよい。

【0183】

上記図16の例では、セキュリティモジュール23とメモリ記録再生装置200において、手順R42, R43のように、自己が保持しているリボケーションリスト内にそれぞれ相手方のIDが掲載されているか否かの検証を行った後、手順R44, R45にてリボケーションリストのバージョンナンバーの新旧をチェックし、新しいバージョンのリボケーションリストで古いバージョンのリボケーションリストを更新する例を挙げたが、以下に説明するように、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方のIDが掲載されているか否かを検証するようにしてもよい。この場合、必ず新しいバージョンのリボケーションリストによって相手方のIDがチェックされるため、より確実に不正なものであるか否かを判定できる。なお、両者のリボケーションリストのバージョンナンバーが同じ場合もあり得るので、以下の説明では、バージョンナンバーが同じ場合も考慮して説明する。

【0184】

図17には、第2の実施の形態において、上述のように先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方のIDを検証するようにした場合の、データ記録時の手順を示す。

【0185】

なお、図17の手順R51～手順R56までは、前述した第1の実施の形態における図8の手順R21～手順R26までと略々同じである。

【0186】

この図17において、メモリ記録再生装置200は、手順R51として、乱数 R_B を記録コマンドと共にセキュリティモジュール23に送る。上記記録コマンドと乱数 R_B を受け取ったセキュリティモジュール23は、手順R52として、乱数 R_A と K_A を生成し、 $V_A = K_A \cdot G$ の計算を行い、さらに、前記同様に乱数 R_A 、乱数 R_B 、値 V_A 、バージョンナンバー $\text{Rev}V_A$ からなるビット列にデジタル署名を行って Sig_A を生成し、それら R_A , R_B , V_A , $\text{Rev}V_A$, Sig_A と証明書 Cer

t_A をメモリ記録再生装置 200 に送る。

【0187】

上記セキュリティモジュール 23 から $Cert_A$, R_A , R_B , V_A , $RevV_A$, Sig_A を受け取ると、メモリ記録再生装置 200 は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行う。すなわち、メモリ記録再生装置 200 は、証明書 $Cert_A$ の検証を行い、当該検証をパスできないときには、そのセキュリティモジュール 23 を備えたメモリ情報記録媒体 20 を不正な媒体とみなして当該プロトコルを終了し、一方で、証明書 $Cert_A$ の検証において正当であると判定された場合は、上記証明書 $Cert_A$ からパブリック鍵 $PubKey_A$ を手に入れる。次に、メモリ記録再生装置 200 は、セキュリティモジュール 23 から返送されてきた乱数 R_B と先の手順 R51 で生成した乱数 R_B とが等しく、且つデジタル署名 Sig_A が正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール 23 を備えたメモリ情報記録媒体 20 が不正な媒体であると判断して当該プロトコルを終了する。

【0188】

上記メモリ記録再生装置 200 から返送されてきた乱数 R_B と先に生成したもののが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、メモリ記録再生装置 200 は、手順 R53 として、 K_B を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、バージョンナンバー $RevV_B$ となるビット列にデジタル署名を行って Sig_B を生成し、これら R_B , R_A , V_B , $RevV_B$, Sig_B と証明書 $Cert_B$ をセキュリティモジュール 23 に送る。

【0189】

上記メモリ記録再生装置 200 から $Cert_B$, R_B , R_A , V_B , $RevV_B$, Sig_B を受け取ると、セキュリティモジュール 23 は、メモリ記録再生装置 200 の証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行う。すなわち、セキュリティモジュール 23 は、先ず、証明書 $Cert_B$ の検証を行い、当該検証をパスできないときには、そのメモリ記録再生装置 200 を不正な装置とみなして当該プロトコルを終了し、一方で、証明書 $Cert_B$ の検証において正当であると判定された場合には、上記証明書 $Cert_B$ からパブリック鍵 $PubKey_B$ を手に入れる。次に、セキュリティ

モジュール 23 は、メモリ記録再生装置 200 から返送されてきた乱数 R_A と先の手順 R52 で生成した乱数 R_A とが等しく、且つデジタル署名 Sig_B が正当であると判定されたときには、次の処理に進み、そうでない場合にはメモリ記録再生装置 200 が不正な装置であると判断して当該プロトコルを終了する。

【0190】

上述のように、セキュリティモジュール 23 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 23 では $K_A \cdot V_B$ の計算を行い、また、メモリ記録再生装置 200 では $K_B \cdot V_A$ の計算を行い、さらにそれらの x 座標の下位 z ビットをセッション鍵 K_{se} としてこれらセキュリティモジュール 23 とメモリ記録再生装置 200 が共有する。

【0191】

また、セキュリティモジュール 23 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 23 とメモリ記録再生装置 200 は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行う。

【0192】

ここで、両者のバージョンナンバーが同じである場合、メモリ記録再生装置 200 とセキュリティモジュール 23 は、それぞれが保持するリボケーションリストを用いて相手方の ID の検証を行い、互いに相手方の ID がリボケーションリストに掲載されていないことを検証する。当該相互検証の結果、両者において共にリボケーションリストに掲載されていないと判定された場合には、後段の手順 R56 の処理に進む。また、セキュリティモジュール 23 において、メモリ記録再生装置 200 の ID_B が自己のリボケーションリストに掲載されている場合には、当該メモリ記録再生装置 200 は不正な装置であると判定し、当該プロトコルを終了する。同じく、メモリ記録再生装置 200 において、セキュリティモジュール 23 の ID_A が自己のリボケーションリストに掲載されている場合には、当該セキュリティモジュール 23 は不正な媒体のものであると判定し、当該プロトコルを終了する。

【0193】

一方、セキュリティモジュール23とメモリ記録再生装置200においてそれぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順R54又はR55として、上記新しいバージョンのリボケーションリストを相手方に送り、この新しいバージョンのリボケーションリストを受け取った側では当該新しいバージョンのリボケーションリストを用いて相手方のID検証を行うと共に、古いバージョンのリボケーションリストを更新する。

【0194】

すなわち例えば、セキュリティモジュール23のリボケーションリストのバージョンが、~~メモリ記録再生装置200のものよりも新しい場合、セキュリティモジュール23では自己が保持するリボケーションリストを用いてメモリ記録再生装置200のID_Bの検証を行い、その検証の結果、メモリ記録再生装置200がリボケーションリストに記載されていないとき、手順R54として、自己が保持しているリボケーションリストをメモリ記録再生装置200に送る。当該リボケーションリストを受け取ったメモリ記録再生装置200は、当該送られてきた新しいリボケーションリストを用いてセキュリティモジュール23のID_Aの検証を行い、その検証の結果、セキュリティモジュール23のID_Aがリボケーションリストに記載されていないとき、上記セキュリティモジュール23から送られてきた新しいバージョンのリボケーションリスト内に含まれるセンタTCの署名TCSigを検証し、当該署名TCSigが正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新する。一方、署名TCSigが正しくない場合は、当該プロトコルを終了する。~~

【0195】

また、メモリ記録再生装置200のリボケーションリストのバージョンが、セキュリティモジュール23のものよりも新しい場合、メモリ記録再生装置200では自己が保持するリボケーションリストを用いてセキュリティモジュール23のID_Aの検証を行い、その検証の結果、セキュリティモジュール23がリボケーションリストに記載されていないとき、手順R55として、自己が保持してい

るリボケーションリストをセキュリティモジュール 23 に送る。当該リボケーションリストを受け取ったセキュリティモジュール 23 は、その送られてきた新しいリボケーションリストを用いてメモリ記録再生装置 200 の ID_B の検証を行い、その検証の結果、メモリ記録再生装置 200 の ID_B がリボケーションリストに記載されていないとき、上記メモリ記録再生装置 200 から送られてきた新しいバージョンのリボケーションリスト内に含まれるセンタ TC の署名 TC Sig を検証し、当該署名 TC Sig が正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新する。一方、署名 TC Sig が正しくない場合は、当該プロトコルを終了する。

【0196】

次に、メモリ記録再生装置 200 は、手順 R 5 6 として、メモリ情報記録媒体 20 のメモリ部 22 に記録するコンテンツデータを暗号化するための暗号鍵 K_{co} をセッション鍵 K_{se} にて暗号化した値 $Enc(K_{se}, K_{co})$ をセキュリティモジュール 23 に送信する。

【0197】

この時のセキュリティモジュール 23 は、手順 R 5 7 として、上記メモリ記録再生装置 200 から送信されてきた値 $Enc(K_{se}, K_{co})$ をセッション鍵 K_{se} を用いて復号することにより、暗号鍵 K_{co} を復元し、さらに、この暗号鍵 K_{co} を自己が持つストレージ鍵 K_{st} にて暗号化した値 $Enc(K_{st}, K_{co})$ をメモリ部 22 或いは不揮発性メモリ 44 に格納する。

【0198】

その後、メモリ記録再生装置 200 は、手順 R 5 8 として、上記暗号鍵 K_{co} を用いて暗号化したコンテンツデータ $Enc(K_{co}, data)$ をセキュリティモジュール 23 に送る。

【0199】

この時のセキュリティモジュール 23 は、手順 R 5 9 として、当該暗号化されているコンテンツデータ $Enc(K_{co}, data)$ をメモリ部 22 に格納する。なお、上記リボケーションリストの伝送は、上記コンテンツデータの伝送の合間、または終了後に行ってもよい。

【0200】

次に、この第2の実施の形態において、メモリ情報記録媒体20のメモリ部22へのデータの記録処理については、図18のようにすることも可能である。なお、図18の手順R61～R64については、図15の手順R31～R34と同じであるためその説明は省略する。

【0201】

この図18の例において、メモリ記録再生装置200は、手順R65として、前述の認証と鍵共有プロトコルにおいてセキュリティモジュール23と共有したセッション鍵Kseを用いてデータを暗号化し、当該暗号化されたデータEnc(Kse, data)をセキュリティモジュール23に送る。

【0202】

この暗号化されたデータEnc(Kse, data)を受け取ったセキュリティモジュール23は、手順R66として、同じくセッション鍵Kseを用いてこれを復号し、平文のデータを得、次に新たに発生させた暗号鍵Kcoで暗号化した値Enc(Kco, data)をデータ用のメモリ部22に記録する。

【0203】

ここで、セキュリティモジュール23は、暗号鍵Kcoを安全にその内部の不揮発性メモリ44に格納するか、セキュリティモジュール23が予め格納しているストレージ鍵Kstを用いて暗号鍵Kcoを暗号化した値Enc(Kst, Kco)を上記大容量のメモリ部22に格納する。このようにすると、セキュリティモジュール23はデータの暗号鍵Kcoをメモリ記録再生装置200にも教えないで済む（つまり、外部に漏らさない）ようになる。

【0204】

次に、図19～図22を用いて、上記第2の実施の形態のメモリ記録再生装置200がメモリ情報記録媒体20のメモリ部22からデータを再生する手順を説明する。

【0205】

なお、上述したように、第2の実施の形態のメモリ記録再生装置200は、センタTCから与えられたID、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、

及びリボケーションリストを上記不揮発性メモリ210に格納しており、また同様に、当該第2の実施の形態のメモリ情報記録媒体20のセキュリティモジュール23は、センタTCから与えられたID、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを上記不揮発性メモリ44に格納している。また、メモリ記録再生装置200は、再生すべきデータに付与されたレコーディングIDを知っているものとする。

【0206】

先ず、図19において、メモリ記録再生装置200は、手順P31として、メモリ情報記録媒体20のセキュリティモジュール23に対して、これからデータの再生を行うことを示す再生コマンド（再生開始コマンド）と、1回1回の記録を識別するために個別に割り当てるレコーディングIDとを送る。

【0207】

次に、手順P32として、メモリ記録再生装置200及びメモリ情報記録媒体20のセキュリティモジュール23は、上記再生コマンドをトリガーとして、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する。このプロトコルの内容は、前述した第1の実施の形態におけるデータの再生時に用いられるプロトコルと同様であり、それぞれ他方が持つ公開鍵と秘密鍵が正しいことの検証と、リボケーションリストに相手方のIDが載せられていないことの確認を互に行い、セッション鍵K_{se}を共有し、また自分が持つリボケーションリストのバージョンナンバーを送り合う。

【0208】

また、前記図15の手順R33、R34と同様に、図19の手順P33、P34として、どちらかが相対的に新しいリボケーションリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のリボケーションリストを更新することも同様である。すなわち、手順P33には、セキュリティモジュール23上のリボケーションリストのバージョンが、メモリ記録再生装置200上のリボケーションリストのバージョンよりも新しい場合におけるリボケーションリストの流れを示しており、また、手順P34には、メモリ記録再生装置200上のリボケーションリストのバージョンが、セキュリティモジュール23上の

リボケーションリストのバージョンよりも新しい場合におけるリボケーションリストの流れを示している。

【0209】

なお、手順P33, RP4におけるリボケーションリストの送付は、後の手順P35, P36におけるデータの再生と順序が前後してもかまわない。つまり、手順P35, P36にてデータの記録を行った後に、手順P33或いはP34でのリボケーションリストの送付を行うようにしてもよい。

【0210】

次に、データをメモリ情報記録媒体20のメモリ部22から読み出す前に、このデータを暗号化したときの暗号鍵Kcoをメモリ記録再生装置200が知ることが必要になる。

【0211】

暗号鍵Kcoは、セキュリティモジュール23が安全にその内部の不揮発性メモリ44に格納しているか、或いはセキュリティモジュール23が予め格納しているストレージ鍵Kstを用いて当該暗号鍵Kcoを暗号化した値Enc(Kst, Kco)としてメモリ部22に記録されている。

【0212】

前者の場合、セキュリティモジュール23は、不揮発性メモリ44に格納されている暗号鍵Kcoをセッション鍵Kseで暗号化した値Enc(Kse, Kco)を、メモリ記録再生装置200に送る。メモリ記録再生装置200では、当該値Enc(Kse, Kco)をセッション鍵Kseを用いて復号することにより暗号鍵Kcoを得る。

【0213】

一方、後者の場合、セキュリティモジュール23は、手順P35として、メモリ部22から上記ストレージ鍵Kstで暗号鍵Kcoを暗号化した値Enc(Kst, Kco)を読み出し、これをストレージ鍵Kstを用いて復号して暗号鍵Kcoを得る。さらに、この暗号鍵Kcoをセッション鍵Kseで暗号化した値Enc(Kse, Kco)を、手順P36としてメモリ記録再生装置200に送る。メモリ記録再生装置200は、当該値Enc(Kse, Kco)をセッション鍵Kseを用いて復号することにより暗号鍵Kcoを得る。

【0214】

上述のように、メモリ記録再生装置200は、データを暗号化したときの暗号鍵Kcoを得ることができる。

【0215】

その後、メモリ記録再生装置200は、上記メモリ情報記録媒体20のメモリ部22から、上記暗号鍵Kcoを用いて暗号化されているデータEnc(Kco, data)を読み出し、先に取得した暗号鍵Kcoを用いてこれを復号し使用する。

【0216】

以上が、メモリ情報記録媒体20のメモリ部22からデータを読み出す処理の基本的な手順である。

【0217】

次に、図20には、上記第2の実施の形態のメモリ記録再生装置200がメモリ情報記録媒体20からデータを再生するまでの手順の詳細を示す。なお、この図20では、メモリ記録再生装置200に係る各情報について「B」の文字を付し、メモリ情報記録媒体20のセキュリティモジュール23に係る各情報について「A」の文字を付している。上述同様に、メモリ記録再生装置200とセキュリティモジュール23は、センタTCから与えられたID(セキュリティモジュール23のID_A、メモリ記録再生装置200のID_B)、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを、それぞれ対応する不揮発性メモリ210、44に格納している。

【0218】

図20の手順P41～手順P46までは、前述した第1の実施の形態における図10の手順P11～手順P16までと略々同じである。

【0219】

すなわち、メモリ記録再生装置200は、手順P41として乱数R_Bと再生コマンドをセキュリティモジュール23に送る。セキュリティモジュール23は、手順P42として、乱数R_AとK_Aを生成し、 $V_A = K_A \cdot G$ の計算を行い、乱数R_A、乱数R_B、値V_A、バージョンナンバーRevV_Aからなるビット列にデジタル署名を行ってSig_Aを得、これらに証明書Cert_Aを加えてメモリ記録再生装置20

0に送る。なお、セキュリティモジュール23がリボケーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして0を用いる。

【0220】

次に、メモリ記録再生装置200は、証明書 $Cert_A$ の検証を行い、その検証をパスできないときには、そのメモリ情報記録媒体20を不正な媒体とみなして当該プロトコルを終了し、一方、当該検証において正当であると判定された場合、上記証明書 $Cert_A$ からパブリック鍵 $PubKey_A$ を手に入れる。次に、メモリ記録再生装置200は、セキュリティモジュール23から返送されてきた乱数 R_B と先の手順P41で生成した乱数 R_B とが等しく、且つデジタル署名 Sig_A が正当であると判定されたときには、次の処理に進み、そうでない場合には上記メモリ情報記録媒体20が不正な媒体であると判断して当該プロトコルを終了する。

【0221】

上記セキュリティモジュール23から返送されたきた乱数 R_B と先に生成したものとが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、メモリ記録再生装置200は、自己が保持しているリボケーションリストを用い、上記メモリ情報記録媒体20の ID_A が当該リボケーションリストに掲載されていないことを検証し、この検証の結果、上記 ID_A がリボケーションリストに掲載されている場合には、当該メモリ情報記録媒体20は不正な媒体であると判定し、当該プロトコルを終了する。一方、上記 ID_A が当該リボケーションリストに掲載されていない場合、メモリ記録再生装置200は、手順P43として、 K_B を生成して $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、バージョンナンバー $RevV_B$ からなるビット列にデジタル署名を行って Sig_B を得、それらに証明書 $Cert_B$ を加えてセキュリティモジュール23に送る。なお、メモリ記録再生装置200がリボケーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして0を用いる。

【0222】

次に、セキュリティモジュール23は、上記証明書 $Cert_B$ の検証を行い、当該検証をパスできないときには、そのメモリ記録再生装置200を不正な装置とみなして当該プロトコルを終了し、一方、当該検証において正当であると判定され

た場合は、上記証明書 $Cert_B$ からパブリック鍵 $PubKey_B$ を手に入れる。次に、セキュリティモジュール 2 3 は、メモリ記録再生装置 2 0 0 から返送されてきた乱数 R_A と先に手順 P 4 2 で生成した乱数 R_A とが等しく、且つデジタル署名 Sig_B が正当であると判定されたときには、次の処理に進み、そうでない場合にはメモリ記録再生装置 2 0 0 が不正な装置であると判断して当該プロトコルを終了する。

【 0 2 2 3 】

上記メモリ記録再生装置 2 0 0 から返送されてきた乱数 R_A と先に生成したものが等しく、且つデジタル署名 Sig_B が正当であると判定されたとき、セキュリティモジュール 2 3 は、自己が保持するリボケーションリストを用い、上記 ID_B が当該リボケーションリストに掲載されていないことを検証し、その検証の結果、上記 ID_B がリボケーションリストに掲載されている場合には、当該メモリ記録再生装置 2 0 0 は不正な装置であると判定し、当該プロトコルを終了する。

【 0 2 2 4 】

一方、上記 ID_B がリボケーションリストに掲載されていない場合、すなわち、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 は、セッション鍵 K_{se} を生成して共有する。

【 0 2 2 5 】

次に、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順 P 4 4 又は P 4 5 として、その新しいバージョンのリボケーションリストを相手方に送る。このように、相手方から新しいバージョンナンバーのリボケーションリストが送られてきた方は、センタ TC の署名 TC_{Sig} を検証し、当該署名 TC_{Sig} が正しい場合、その新しいリボケーションリストを用いた更新を行い、一方で、署名 TC_{Sig} が正しくない場合は、当該プロトコルを終了する。

【0226】

次に、暗号鍵 K_{co} を暗号化した値 $E_{nc}(K_{st}, K_{co})$ が、例えばメモリ情報記録媒体 20 のメモリ部 22 に格納されているとした場合は、セキュリティモジュール 23 は、手順 P46 として、上記メモリ部 22 から上記読み出した値 $E_{nc}(K_{st}, K_{co})$ をストレージ鍵 K_{st} を用いて復号して暗号鍵 K_{co} を得、さらに、この暗号鍵 K_{co} をセッション鍵 K_{se} で暗号化した値 $E_{nc}(K_{se}, K_{co})$ を、手順 P57 としてメモリ記録再生装置 200 に送る。メモリ記録再生装置 200 は、当該値 $E_{nc}(K_{se}, K_{co})$ をセッション鍵 K_{se} を用いて復号することにより暗号鍵 K_{co} を得る。

【0227】

その後、セキュリティモジュール 23 は、手順 P48 として、暗号化されているコンテンツデータ $E_{nc}(K_{co}, data)$ をメモリ情報記録媒体 20 のメモリ部 22 から読み出し、このデータ $E_{nc}(K_{co}, data)$ をメモリ記録再生装置 200 に送信する。メモリ記録再生装置 200 では、先に取得した暗号鍵 K_{co} を用いて、上記データ $E_{nc}(K_{co}, data)$ を復号する。

【0228】

なお、上記リボケーションリストの伝送は、上記コンテンツデータの伝送の間、または終了後に行ってもよい。

【0229】

次に、図 21 には、第 2 の実施の形態においてデータの再生を行う場合において、前記第 1 の実施の形態の図 11 の例と同様に、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方の ID が掲載されているか否かを検証するようにしたときの手順を示す。

【0230】

なお、図 21 の手順 P51～手順 P55 までは、前述した第 1 の実施の形態における図 11 の手順 P21～手順 R25 までと略々同じである。

【0231】

この図 21 において、メモリ記録再生装置 200 は、手順 P51 として、乱数

R_B を再生コマンドと共にセキュリティモジュール23に送る。上記再生コマンドと乱数 R_B を受け取ったセキュリティモジュール23は、手順P52として、乱数 R_A と K_A を生成し、 $V_A = K_A \cdot G$ の計算を行い、さらに、前記同様に乱数 R_A 、乱数 R_B 、値 V_A 、バージョンナンバー $\text{Rev}V_A$ からなるビット列にデジタル署名を行って Sig_A を生成し、それら R_A 、 R_B 、 V_A 、 $\text{Rev}V_A$ 、 Sig_A と証明書 Cert_A をメモリ記録再生装置200に送る。

【0232】

上記セキュリティモジュール23から Cert_A 、 R_A 、 R_B 、 V_A 、 $\text{Rev}V_A$ 、 Sig_A を受け取ると、メモリ記録再生装置200は、証明書 Cert_A 、デジタル署名 Sig_A の検証を行う。上記証明書 Cert_A の検証をパスできないときには、メモリ記録再生装置200は、メモリ情報記録媒体20を不正な媒体とみなして当該プロトコルを終了し、一方で、当該検証において正当であると判定された場合は上記証明書 Cert_A からパブリック鍵 PubKey_A を手に入れる。次に、メモリ記録再生装置200は、セキュリティモジュール23から返送されてきた乱数 R_B と先の手順R51で生成した乱数 R_B とが等しく、且つデジタル署名 Sig_A が正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール23を備えたメモリ情報記録媒体20が不正な媒体であると判断して当該プロトコルを終了する。

【0233】

上記セキュリティモジュール23から返送されてきた乱数 R_B と先に生成したものとが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、メモリ記録再生装置200は、手順P53として、 K_B を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、バージョンナンバー $\text{Rev}V_B$ からなるビット列にデジタル署名を行って Sig_B を生成し、これら R_B 、 R_A 、 V_B 、 $\text{Rev}V_B$ 、 Sig_B と証明書 Cert_B をセキュリティモジュール23に送る。

【0234】

上記メモリ記録再生装置200から Cert_B 、 R_B 、 R_A 、 V_B 、 $\text{Rev}V_B$ 、 Sig_B を受け取ると、セキュリティモジュール23は、メモリ記録再生装置200の証明書 Cert_B 、デジタル署名 Sig_B の検証を行う。上記証明書 Cert_B の検証をパス

できないとき、セキュリティモジュール 23 は、そのメモリ記録再生装置 200 を不正な装置とみなして当該プロトコルを終了し、一方で、当該検証で正当であると判定した場合には、上記証明書 $Cert_B$ からパブリック鍵 $PubKey_B$ を手に入れる。次に、セキュリティモジュール 23 は、メモリ記録再生装置 200 から返送されてきた乱数 R_A と先の手順 R 52 で生成した乱数 R_A とが等しく、且つデジタル署名 Sig_B が正当であると判定されたときには、次の処理に進み、そうでない場合にはメモリ記録再生装置 200 が不正な装置であると判断して当該プロトコルを終了する。

【0235】

上述のように、セキュリティモジュール 23 とメモリ記録再生装置 200 の両者が共に正当であると検証された場合、セキュリティモジュール 23 とメモリ記録再生装置 200 は、前記セッション鍵 K_{se} を生成して共有する。

【0236】

また、セキュリティモジュール 23 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 213 とメモリ記録再生装置 200 は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行う。

【0237】

ここで、両者のバージョンナンバーが同じである場合、メモリ記録再生装置 200 とセキュリティモジュール 23 は、それぞれが保持するリボケーションリストを用いて相手方の ID の検証を行い、互いに相手方の ID がリボケーションリストに掲載されていないことを検証する。

【0238】

一方、セキュリティモジュール 23 とメモリ記録再生装置 200 においてそれぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順 P 54 又は P 55 として、上記新しいバージョンのリボケーションリストを相手方に送り、この新しいバージョンのリボケーションリストを受け取った側では当該新しいバージョンのリボケーションリストを用いて相手方の

I D 検証を行うと共に、古いバージョンのリボケーションリストを更新する。

【 0 2 3 9 】

手順 P 5 6 ~ P 5 9 は、図 2 0 の手順 P 4 6 ~ P 4 9 と同じであるためその説明は省略する。

【 0 2 4 0 】

次に、当該第 2 の実施の形態におけるデータ再生の手順として、図 2 2 に示すように、図 1 8 に示したデータ記録時の手順に準ずる手順を用いることも可能である。なお、図 2 1 の手順 P 6 1 ~ P 6 4 については、図 1 9 の手順 P 3 1 ~ P 3 4 と同じであるためその説明は省略する。

【 0 2 4 1 】

この図 2 2 の例において、セキュリティモジュール 2 3 は、手順 P 6 5 として、メモリ部 2 2 から読み取った前記暗号化されているコンテンツデータ Enc (Kco, data) を、暗号鍵 Kco を用いて復号し、その復号後のデータをセッション鍵 Kse を用いて暗号化する。セキュリティモジュール 2 3 は、当該セッション鍵 Kse を用いて暗号化されたコンテンツデータ Enc (Kse, data) を、手順 P 6 6 として、メモリ記録再生装置 2 0 0 に送信する。

【 0 2 4 2 】

メモリ記録再生装置 2 0 0 は、上記データ Enc (Kse, data) を、自己が保持するセッション鍵 Kse にて復号する。これにより、メモリ記録再生装置 2 0 0 は、復号後のコンテンツデータを得る。

【 0 2 4 3 】

このようにすることで、セキュリティモジュール 2 3 はデータを暗号化している暗号鍵 Kco をメモリ記録再生装置 2 0 0 に教える必要がなくなる（暗号鍵 Kco が外部に出力することがなくなる）。

【 0 2 4 4 】

以上説明した第 1、第 2 の実施の形態では、秘密鍵が露呈してしまった情報記録媒体或いは記録再生装置の I D（リボークされる機器又は媒体の I D）のリストを用いて、不正に情報が複製等されることを防止した例を挙げたが、本発明では、正当な情報記録媒体或いは記録再生装置を示すレジストレーションリストを

用いることで、上述同様に不正に情報が複製等されることを防止することも可能である。

【0 2 4 5】

すなわち、レジストレーションリストは、登録リスト、正直者リストとも呼ばれ、システム全体若しくはその中の一部であるサブシステムにおいて、正当な情報記録媒体もしくは記録再生装置であるとセンタTCが判断したもののIDをリストアップし、それにデジタル署名を施したものである。

【0 2 4 6】

当該レジストレーションリストは、図23に示すように、例えば単調増加する番号であって当該レジストレーションリストのバージョンを示すバージョンナンバーと、正当な情報記録媒体或いは記録再生装置のID（登録された機器又は媒体のID）のリストと、センタTCによるデジタル署名とからなるものである。このレジストレーションリストの登録は、一例として、あるホームネットワーク内の装置および記録媒体のIDを、そのネットワーク内の一つの装置がリストアップしてセンタTCに送信し、センタTCがこれらの全ての記録媒体及び装置が正当なものであると判断したとき、このリストに対しデジタル署名を付加して送り返し、これを受け取った装置がホームネットワーク内にこのリストを配布するようなことにより行われる。これにより、そのホームネットワーク内で信頼できる装置及び記録媒体全てのIDを各装置と記録媒体は知ることができるようになり、当該レジストレーションリストにリストアップされているIDを持つエンティティ（装置や媒体）のみを信用してプロトコルを行うことが可能となる。言い換えれば、秘密鍵が露呈してしまった記録媒体又は装置、及びそれを用いて不正に複製された記録媒体又は不正に製造された装置については、レジストレーションリストに掲載されないことになり、したがってそれら不正な装置や媒体をこのシステムから排除することが可能になる。また、記録再生装置を工場から出荷する際には、最新版のレジストレーションリストを不揮発性メモリに格納して出荷する。

【0 2 4 7】

以下、上記レジストレーションリストを使用した第3の実施の形態について説

明する。

【0248】

第3の実施の形態は、前述の第1の実施の形態で説明した光ディスク情報記録媒体10のセキュリティモジュール13の不揮発性メモリ34と、光ディスク記録再生装置100の不揮発性メモリ110に、前記リボケーションリストに代えて上記レジストレーションリストを格納するようにした例である。当該第3の実施の形態における光ディスク情報記録媒体10、光ディスク記録再生装置100の構成は、前記図1～図3と同じであるため、それら構成についての説明は省略する。

【0249】

図24から図26を用いて、第3の実施の形態の光ディスク記録再生装置100が光ディスク情報記録媒体10にデータを記録する手順を説明する。なお、図24～図26は、前記第1の実施の形態の図6～図8と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図6～図8とは異なる部分のみ説明する。

【0250】

図24は前記図6と略々同様な手順を表しており、手順R2として、光ディスク記録再生装置100とセキュリティモジュール13との間でレジストレーションリストのバージョンナンバーを交換する。

【0251】

また、手順R3、R4では、何れかの一方が他方のレジストレーションリストより新しいレジストレーションリストを持っていた場合、当該新しいレジストレーションリストを持っている方は自分のレジストレーションリストを他方に送る。一方、古いレジストレーションリストを持っている方は、新しいレジストレーションリストを持っている方から、当該新しいレジストレーションリストを送ってもらい、その正当性を検証した後、自分が持つレジストレーションリストを、その送られてきた新しいレジストレーションリストに更新する。

【0252】

なお、手順R3、R4におけるレジストレーションリストの送付は、後の手順

R 5におけるデータの記録と順序が前後してもかまわない。つまり、手順R 5にてデータの記録を行った後に、手順R 3 或いはR 4でのレジストレーションリストの送付を行うようにしてもよい。

【0 2 5 3】

次に、図 2 5 には、上記図 2 4 に示した第 3 の実施の形態の光ディスク記録再生装置 1 0 0 が光ディスク情報記録媒体 1 0 にデータを記録するまでの手順の詳細を示しており、前記図 7 と略々同様な手順となっている。

【0 2 5 4】

この図 2 5 において、手順R 1 2の際のセキュリティモジュール 1 3 は、乱数 R_A 、乱数 R_B 、値 V_A 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列 $R_A || R_B || V_A || RegV_A$ にデジタル署名の関数 $Sign$ を用いたデジタル署名を行い $Sig_A = Sign(PriKey_A, R_A || R_B || V_A || RegV_A)$ を得る。セキュリティモジュール 1 3 は、これら R_A 、 R_B 、 V_A 、 $RegV_A$ 、 Sig_A に証明書 $Cert_A$ を付け、光ディスク記録再生装置 1 0 0 に送る。なお、セキュリティモジュール 1 3 がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして 0 を用いる。

【0 2 5 5】

これら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RegV_A$ 、 Sig_A を受け取った光ディスク記録再生装置 1 0 0 は、証明書 $Cert_A$ 、デジタル署名 Sig_A 、 ID_A の検証を行い、その検証をパスし、さらに、セキュリティモジュールから返送されてきた乱数 R_B と先に生成したものとが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、自己の不揮発性メモリ 1 1 0 に格納しているレジストレーションリストを用い、光ディスク情報記録媒体 1 0 の ID_A が当該レジストレーションリストに登録されていることを検証する。この検証の結果、光ディスク情報記録媒体 1 0 の ID_A がレジストレーションリストに登録されていない場合には、当該光ディスク情報記録媒体 1 0 は不正な媒体であると判定し、当該プロトコルを終了する。

【0 2 5 6】

一方、上記 ID_A が当該レジストレーションリストに登録されており、その光

ディスク情報記録媒体 10 が正当であると判断した場合、光ディスク記録再生装置 100 は、手順 R13 として、 K_B を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、当該装置 100 が持つレジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列 $R_B || R_A || V_B || RegV_B$ にデジタル署名を行って $Sig_B = \text{Sign}(\text{PriKey}_B, R_B || R_A || V_B || RegV_B)$ を得る。光ディスク記録再生装置 100 は、これら R_B 、 R_A 、 V_B 、 $RegV_B$ 、 Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール 13 に送る。なお、光ディスク記録再生装置 100 がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして 0 を用いる。

【0257】

上記光ディスク記録再生装置 100 から $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RegV_B$ 、 Sig_B を受け取ると、セキュリティモジュール 13 は、証明書 $Cert_B$ 、デジタル署名 Sig_B 、 ID_B の検証を行い、その検証をパスした時、自己の不揮発性メモリ 34 に格納しているレジストレーションリストを用い、光ディスク記録再生装置 100 の ID_B が当該レジストレーションリストに登録されていることを検証する。この検証の結果、光ディスク記録再生装置 100 の ID_B がレジストレーションリストに登録されていない場合には、当該光ディスク記録再生装置 100 は不正な装置であると判定し、当該プロトコルを終了する。

【0258】

一方、光ディスク記録再生装置 100 の ID_B が当該レジストレーションリストに登録されており、その光ディスク記録再生装置 100 が正当であると判断した場合、すなわち、セキュリティモジュール 13 と光ディスク記録再生装置 100 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 13 と光ディスク記録再生装置 100 はセッション鍵 K_{se} を生成して共有する。

【0259】

次に、セキュリティモジュール 13 と光ディスク記録再生装置 100 は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順 R14 又は

R 1 5として、その新しいバージョンのレジストレーションリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのレジストレーションリストが送られてきた方は、当該レジストレーションリスト内に含まれるセンタTCの署名TCSigを検証し、その検証をパスしたとき、その新しいレジストレーションリストを用いて自己が保持している古いレジストレーションリストを更新（リストのアップデート）する。

【0 2 6 0】

その後の手順R 1 6以降は、前記図 7 の場合と同様である。

【0 2 6 1】

なお、上記レジストレーションリストの伝送は、コンテンツデータの伝送の間、または終了後に行ってもよい。

【0 2 6 2】

図 2 6 には、前記第 1 の実施の形態における図 8 の手順を、レジストレーションリストにも適用した例を示している。すなわち、図 2 6 は、先にレジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のレジストレーションリストを用いて相手方のIDを検証するようにした場合の、データ記録時の手順を示している。

【0 2 6 3】

この図 2 6 において、手順R 2 2の際のセキュリティモジュール 1 3 は、乱数 R_A 、乱数 R_B 、値 V_A 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列 $R_A || R_B || V_A || RegV_A$ にデジタル署名を行って Sig_A を得、これら R_A 、 R_B 、 V_A 、 $RegV_A$ 、 Sig_A に証明書 $Cert_A$ を付けて光ディスク記録再生装置 1 0 0 に送る。

【0 2 6 4】

これら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RegV_A$ 、 Sig_A を受け取った光ディスク記録再生装置 1 0 0 は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 1 3 から返送されてきた乱数 R_B と先に生成したもののが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順R 2 3として、 K_B を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、

上記乱数 R_B 、乱数 R_A 、値 V_B 、当該装置 100 が持つレジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って Sig_B を得る。光ディスク記録再生装置 100 は、これら R_B 、 R_A 、 V_B 、 $RegV_B$ 、 Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール 13 に送る。

【0265】

上記光ディスク記録再生装置 100 から $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RegV_B$ 、 Sig_B を受け取ると、セキュリティモジュール 13 は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行い、その検証をパスした時、次の処理に進む。

【0266】

上述のように、セキュリティモジュール 13 と光ディスク記録再生装置 100 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 13 と光ディスク記録再生装置 100 は、セッション鍵 K_{se} を生成して共有する。

【0267】

また、セキュリティモジュール 13 と光ディスク記録再生装置 100 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 13 と光ディスク記録再生装置 100 は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行う。

【0268】

ここで、両者のバージョンナンバーが同じである場合、光ディスク記録再生装置 100 とセキュリティモジュール 13 は、それぞれが保持するレジストレーションリストを用いて相手方の ID の検証を行い、互いに相手方の ID がレジストレーションリストに登録されていることを検証する。このレジストレーションリストの相互検証の結果、両者において共にレジストレーションリストに登録されていると判定された場合には、後段の手順 R26 の処理に進む。また、セキュリティモジュール 13 において、光ディスク記録再生装置 100 の ID_B が自己のレジストレーションリストに登録されていない場合には、当該光ディスク記録再生装置 100 は不正な装置であると判定し、当該プロトコルを終了する。同じく、光ディスク記録再生装置 100 において、セキュリティモジュール 13 の ID

A が自己のレジストレーションリストに登録されていない場合には、当該セキュリティモジュール 1 3 は不正な媒体のものであると判定し、当該プロトコルを終了する。

【0 2 6 9】

一方、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 においてそれぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順 R 2 4 又は R 2 5 として、上記新しいバージョンのレジストレーションリストを相手方に送り、この新しいバージョンのレジストレーションリストを受け取った側では当該新しいバージョンのレジストレーションリストを用いて相手方の ID 検証を行うと共に、古いバージョンのレジストレーションリストを更新する。

【0 2 7 0】

その後の手順 R 2 6 以降は、前記図 8 の場合と同様である。

【0 2 7 1】

次に、図 2 7 ~ 図 2 9 を用いて、上記第 3 の実施の形態の光ディスク記録再生装置 1 0 0 が光ディスク 1 2 からデータを再生する手順を説明する。なお、図 2 7 ~ 図 2 6 は、前記第 1 の実施の形態の図 9 ~ 図 1 1 と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図 9 ~ 図 1 1 とは異なる部分のみ説明する。

【0 2 7 2】

図 2 7 において、光ディスク記録再生装置 1 0 0 とセキュリティモジュール 1 3 は、手順 P 2 にて、レジストレーションリストに相手方の ID が載せられていないことの確認を互に行い、自分が持つレジストレーションリストのバージョンナンバーを送り合う。

【0 2 7 3】

また、手順 P 3, P 4 として、光ディスク記録再生装置 1 0 0 とセキュリティモジュール 1 3 は、どちらかが相対的に新しいレジストレーションリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のレジスト

レーションリストを更新することも同様である。

【0274】

その後の手順P5以降は、前記図9の場合と同様である。

【0275】

次に、図28には、上記図27に示した第3の実施の形態の光ディスク記録再生装置100が光ディスク情報記録媒体10からデータを再生するまでの手順の詳細を示している。なお、当該図28の手順は、前記図10と略々同様な手順となっている。

【0276】

この図28において、手順P12の際のセキュリティモジュール13は、乱数 R_A 、乱数 R_B 、値 V_A 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列にデジタル署名を行い Sig_A を得る。セキュリティモジュール13は、これらに証明書 $Cert_A$ を付け、光ディスク記録再生装置100に送る。なお、セキュリティモジュール13がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして0を用いる。

【0277】

これら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RegV_A$ 、 Sig_A を受け取った光ディスク記録再生装置100は、証明書 $Cert_A$ 、デジタル署名 Sig_A 、 ID_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール13から返送されてきた乱数 R_B と先に生成したものが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、自己の不揮発性メモリ110に格納しているレジストレーションリストを用い、光ディスク情報記録媒体10の ID_A が当該レジストレーションリストに登録されていることを検証する。この検証の結果、光ディスク情報記録媒体10の ID_A がレジストレーションリストに登録されていない場合には、当該光ディスク情報記録媒体10は不正な媒体であると判定し、当該プロトコルを終了する。

【0278】

一方、上記 ID_A が当該レジストレーションリストに登録されており、その光ディスク情報記録媒体10が正当であると判断した場合、光ディスク記録再生装

置 1 0 0 は、手順 P 1 3 として、 K_B を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、当該装置 1 0 0 のレジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って Sig_B を得る。光ディスク記録再生装置 1 0 0 は、これら R_B 、 R_A 、 V_B 、 $RegV_B$ 、 Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール 1 3 に送る。なお、光ディスク記録再生装置 1 0 0 がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして 0 を用いる。

【0 2 7 9】

上記光ディスク記録再生装置 1 0 0 から $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RegV_B$ 、 Sig_B を受け取ると、セキュリティモジュール 1 3 は、証明書 $Cert_B$ 、デジタル署名 Sig_B 、 ID_B の検証を行い、その検証をパスした時、自己の不揮発性メモリ 3 4 に格納しているレジストレーションリストを用い、光ディスク記録再生装置 1 0 0 の ID_B が当該レジストレーションリストに登録されていることを検証する。この検証の結果、光ディスク記録再生装置 1 0 0 の ID_B がレジストレーションリストに登録されていない場合には、当該光ディスク記録再生装置 1 0 0 は不正な装置であると判定し、当該プロトコルを終了する。

【0 2 8 0】

一方、光ディスク記録再生装置 1 0 0 の ID_B が当該レジストレーションリストに登録されており、その光ディスク記録再生装置 1 0 0 が正当であると判断した場合、すなわち、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 はセッション鍵 K_{se} を生成して共有する。

【0 2 8 1】

次に、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順 P 1 4 又は P 1 5 として、その新しいバージョンのレジストレーションリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのレジストレーション

リストが送られてきた方は、当該レジストレーションリスト内に含まれるセンタ TC の署名 $TC\text{Sig}$ を検証し、その検証をパスしたとき、その新しいレジストレーションリストを用いて自己が保持している古いレジストレーションリストを更新（リストのアップデート）する。

【0282】

その後の手順 P 16 以降は、前記図 10 の場合と同様である。

【0283】

なお、上記レジストレーションリストの伝送は、コンテンツデータの伝送の間、または終了後に行ってもよい。

【0284】

図 29 には、前記第 1 の実施の形態における図 1-1 の手順を、レジストレーションリストにも適用した例を示している。すなわち、図 29 は、先にレジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のレジストレーションリストを用いて相手方の ID を検証するようにした場合の、データ再生時の手順を示している。

【0285】

この図 29 において、手順 P 22 の際のセキュリティモジュール 13 は、乱数 R_A 、乱数 R_B 、値 V_A 、レジストレーションリストのバージョンナンバー $\text{Reg}V_A$ からなるビット列にデジタル署名を行って Sig_A を得、これらに証明書 Cert_A を付けて光ディスク記録再生装置 100 に送る。

【0286】

それらを受け取った光ディスク記録再生装置 100 は、証明書 Cert_A 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 13 から返送されてきた乱数 R_B と先に生成したものとが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順 P 23 として、 K_B を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、当該装置 100 が持つレジストレーションリストのバージョンナンバー $\text{Reg}V_B$ からなるビット列にデジタル署名を行って Sig_B を得る。光ディスク記録再生装置 100 は、これら R_B 、 R_A 、 V_B 、 $\text{Reg}V_B$ 、 Sig_B に証明書 Cert_B を付け、セキュリティ

モジュール 13 に送る。上記光ディスク記録再生装置 100 から $Cert_B$, R_B , R_A , V_B , $RegV_B$, Sig_B を受け取ると、セキュリティモジュール 13 は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行い、その検証をパスした時、次の処理に進む。

【0287】

セキュリティモジュール 13 と光ディスク記録再生装置 100 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 13 と光ディスク記録再生装置 100 は、セッション鍵 K_{se} を生成して共有する。また、セキュリティモジュール 13 と光ディスク記録再生装置 100 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 13 と光ディスク記録再生装置 100 は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行う。

【0288】

両者のバージョンナンバーが同じである場合、光ディスク記録再生装置 100 とセキュリティモジュール 13 は、それぞれが保持するレジストレーションリストを用いて相手方の ID の検証を行い、互いに相手方の ID がレジストレーションリストに登録されていることを検証する。このレジストレーションリストの相互検証の結果、両者において共にレジストレーションリストに登録されていると判定された場合には、後段の手順 P26 の処理に進む。また、セキュリティモジュール 13 において、光ディスク記録再生装置 100 の ID_B が自己のレジストレーションリストに登録されていない場合には、当該光ディスク記録再生装置 100 は不正な装置であると判定し、当該プロトコルを終了する。同じく、光ディスク記録再生装置 100 において、セキュリティモジュール 13 の ID_A が自己のレジストレーションリストに登録されていない場合には、当該セキュリティモジュール 13 は不正な媒体のものであると判定し、当該プロトコルを終了する。

【0289】

一方、セキュリティモジュール 13 と光ディスク記録再生装置 100 においてそれぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバー

ジョンが新しい場合、手順 P 2 4 又は P 2 5 として、上記新しいバージョンのレジストレーションリストを相手方に送り、この新しいバージョンのレジストレーションリストを受け取った側では当該新しいバージョンのレジストレーションリストを用いて相手方の ID 検証を行うと共に、古いバージョンのレジストレーションリストを更新する。

【 0 2 9 0 】

その後の手順 P 2 6 以降は、前記図 1 1 の場合と同様である。

【 0 2 9 1 】

次に、本発明の第 4 の実施の形態について説明する。

【 0 2 9 2 】

~~第 4 の実施の形態は、前述の第 2 の実施の形態で説明したメモリ情報記録媒体~~
2 0 のセキュリティモジュール 2 3 の不揮発性メモリ 4 4 と、メモリ記録再生装置 2 0 0 の不揮発性メモリ 2 1 0 に、前記リボケーションリストに代えて上記レジストレーションリストを格納するようにした例である。当該第 4 の実施の形態におけるメモリ情報記録媒体 2 0、メモリ記録再生装置 2 0 0 の構成は、前記図 1 2 ～図 1 4 と同じであるため、それら構成についての説明は省略する。

【 0 2 9 3 】

図 3 0 ～図 3 4 を用いて、第 4 の実施の形態のメモリ記録再生装置 2 0 0 がメモリ情報記録媒体 2 0 にデータを記録する手順を説明する。なお、図 3 0 ～図 3 4 は、前記第 2 の実施の形態の図 1 5 ～図 1 8 と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図 1 5 ～図 1 8 とは異なる部分のみ説明する。

【 0 2 9 4 】

図 3 0 は前記図 1 5 と略々同様な手順を表しており、手順 R 3 2 として、メモリ記録再生装置 2 0 0 とセキュリティモジュール 2 3 との間でレジストレーションリストのバージョンナンバーを交換する。

【 0 2 9 5 】

また、手順 R 3 3、R 3 4 では、何れかの一方が他方のレジストレーションリストより新しいレジストレーションリストを持っていた場合、当該新しいレジス

トレーションリストを持っている方は自分のレジストレーションリストを他方に送る。一方、古いレジストレーションリストを持っている方は、新しいレジストレーションリストを持っている方から、当該新しいレジストレーションリストを送ってもらい、その正当性を検証した後、自分が持つレジストレーションリストを、その送られてきた新しいレジストレーションリストに更新する。

【0296】

なお、手順R33、R34におけるレジストレーションリストの送付は、後の手順R5におけるデータの記録と順序が前後してもかまわない。つまり、手順R35にてデータの記録を行った後に、手順R33或いはR34でのレジストレーションリストの送付を行うようにしてもよい。

【0297】

次に、図31には、上記図30に示した第4の実施の形態のメモリ記録再生装置200がメモリ情報記録媒体20にデータを記録するまでの手順の詳細を示しており、前記図16と略々同様な手順となっている。

【0298】

この図31において、手順R42の際のセキュリティモジュール23は、乱数 R_A 、乱数 R_B 、値 V_A 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列にデジタル署名を行い Sig_A を得る。セキュリティモジュール23は、これらに証明書 $Cert_A$ を付け、メモリ記録再生装置200に送る。なお、セキュリティモジュール23がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして0を用いる。

【0299】

それら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RegV_A$ 、 Sig_A を受け取ったメモリ記録再生装置200は、証明書 $Cert_A$ 、デジタル署名 Sig_A 、 ID_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール23から返送されてきた乱数 R_B と先に生成したものとが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、自己の不揮発性メモリ210に格納しているレジストレーションリストを用い、メモリ情報記録媒体20の ID_A が当該レジストレーションリストに登録されていることを検証する。この検証の結果、メモリ情報記録媒体20のI

D_A がレジストレーションリストに登録されていない場合には、当該メモリ情報記録媒体20は不正な媒体であると判定し、当該プロトコルを終了する。

【0300】

一方、上記 ID_A が当該レジストレーションリストに登録されており、そのメモリ情報記録媒体20が正当であると判断した場合、メモリ記録再生装置200は、手順R43として、 K_B を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、当該装置200が持つレジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って Sig_B を得る。メモリ記録再生装置200は、これらに証明書 $Cert_B$ を付け、セキュリティモジュール23に送る。なお、メモリ記録再生装置200がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして0を用いる。

【0301】

上記メモリ記録再生装置200から $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RegV_B$ 、 Sig_B を受け取ると、セキュリティモジュール23は、証明書 $Cert_B$ 、デジタル署名 Sig_B 、 ID_B の検証を行い、その検証をパスした時、自己の不揮発性メモリ44に格納しているレジストレーションリストを用い、メモリ記録再生装置200の ID_B が当該レジストレーションリストに登録されていることを検証する。この検証の結果、メモリ記録再生装置200の ID_B がレジストレーションリストに登録されていない場合には、当該メモリ記録再生装置200は不正な装置であると判定し、当該プロトコルを終了する。

【0302】

一方、メモリ記録再生装置200の ID_B が当該レジストレーションリストに登録されており、そのメモリ記録再生装置200が正当であると判断した場合、すなわち、セキュリティモジュール23とメモリ記録再生装置200の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール23とメモリ記録再生装置200はセッション鍵 K_{se} を生成して共有する。

【0303】

次に、セキュリティモジュール23とメモリ記録再生装置200は、それぞれ

相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順 R 4 4 又は R 4 5 として、その新しいバージョンのレジストレーションリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのレジストレーションリストが送られてきた方は、当該レジストレーションリスト内に含まれるセンタ TC の署名 TC Sig を検証し、その検証をパスしたとき、その新しいレジストレーションリストを用いて自己が保持している古いレジストレーションリストを更新（リストのアップデート）する。

【0304】

その後の手順 R 4 6 以降は、前記図 1 6 の場合と同様である。

【0305】

なお、上記レジストレーションリストの伝送は、コンテンツデータの伝送の間、または終了後に行ってもよい。

【0306】

図 3 2 には、前記第 2 の実施の形態における図 1 7 の手順を、レジストレーションリストにも適用した例を示している。すなわち、図 3 2 は、先にレジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のレジストレーションリストを用いて相手方の ID を検証するようにした場合の、データ記録時の手順を示している。

【0307】

この図 3 2 において、手順 R 5 2 の際のセキュリティモジュール 2 3 は、乱数 R_A 、乱数 R_B 、値 V_A 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列にデジタル署名を行って Sig_A を得、これらに証明書 $Cert_A$ を付けてメモリ記録再生装置 2 0 0 に送る。

【0308】

これら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RegV_A$ 、 Sig_A を受け取ったメモリ記録再生装置 2 0 0 は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 2 3 から返送されてきた乱数 R_B と先に生成したものが等しく、且つデジタル署名 Sig_A が正当であると判定されたと

き、手順 R 5 3 として、 K_B を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、当該装置 2 0 0 が持つレジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って Sig_B を得る。メモリ記録再生装置 2 0 0 は、これら R_B 、 R_A 、 V_B 、 $RegV_B$ 、 Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール 2 3 に送る。

【0309】

上記メモリ記録再生装置 2 0 0 から $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RegV_B$ 、 Sig_B を受け取ると、セキュリティモジュール 2 3 は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行い、その検証をパスした時、次の処理に進む。

【0310】

上述のように、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 は、セッション鍵 K_{se} を生成して共有する。

【0311】

また、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行う。

【0312】

ここで、両者のバージョンナンバーが同じである場合、メモリ記録再生装置 2 0 0 とセキュリティモジュール 2 3 は、それぞれが保持するレジストレーションリストを用いて相手方の ID の検証を行い、互いに相手方の ID がレジストレーションリストに登録されていることを検証する。このレジストレーションリストの相互検証の結果、両者において共にレジストレーションリストに登録されていると判定された場合には、後段の手順 R 5 6 の処理に進む。また、セキュリティモジュール 2 3 において、メモリ記録再生装置 2 0 0 の ID_B が自己のレジストレーションリストに登録されていない場合には、当該メモリ記録再生装置 2 0 0 は不正な装置であると判定し、当該プロトコルを終了する。同じく、メモリ記録再生装置 2 0 0 において、セキュリティモジュール 2 3 の ID_A が自己のレジス

トレーションリストに登録されていない場合には、当該セキュリティモジュール 2 3 は不正な媒体のものであると判定し、当該プロトコルを終了する。

【0 3 1 3】

一方、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 においてそれぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順 R 5 4 又は R 5 5 として、上記新しいバージョンのレジストレーションリストを相手方に送り、この新しいバージョンのレジストレーションリストを受け取った側では当該新しいバージョンのレジストレーションリストを用いて相手方の I D 検証を行うと共に、古いバージョンのレジストレーションリストを更新する。

【0 3 1 4】

その後の手順 R 5 6 以降は、前記図 1 7 の場合と同様である。

【0 3 1 5】

次に、この第 4 の実施の形態において、メモリ情報記録媒体 2 0 のメモリ部 2 2 へのデータの記録処理については、前述の図 1 8 と同様の図 3 3 に示すような手順とすることも可能である。

【0 3 1 6】

この図 3 3 において、メモリ記録再生装置 2 0 0 とセキュリティモジュール 2 3 は、手順 R 6 2 にて相互にレジストレーションリストのバージョンナンバーを交換する。

【0 3 1 7】

また、手順 R 6 3、R 6 4 では、レジストレーションリストのバージョンナンバーが古い方を、新しいバージョンナンバーのレジストレーションリストにて更新する。

【0 3 1 8】

手順 R 6 5 以降の処理は、前記図 1 8 と同様である。

【0 3 1 9】

次に、図 3 4 ～図 3 7 を用いて、上記第 4 の実施の形態のメモリ記録再生装置

200がメモリ情報記録媒体20のメモリ部22からデータを再生する手順を説明する。なお、図34～図37は、前記第2の実施の形態の図19～図22と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図19～図22とは異なる部分のみ説明する。

【0320】

図34において、メモリ記録再生装置200とセキュリティモジュール23は、手順P32にて、レジストレーションリストに相手方のIDが載せられていないことの確認を互に行い、自分が持つレジストレーションリストのバージョンナンバーを送り合う。

【0321】

また、手順P33、P34として、メモリ記録再生装置200とセキュリティモジュール23は、どちらかが相対的に新しいレジストレーションリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のレジストレーションリストを更新することも同様である。

【0322】

その後の手順P35以降は、前記図19の場合と同様である。

【0323】

次に、図35には、上記図20に示した第2の実施の形態のメモリ記録再生装置200がメモリ情報記録媒体20のメモリ部22からデータを再生するまでの手順の詳細を示している。なお、当該図35の手順は、前記図20と略々同様な手順となっている。

【0324】

この図35において、手順P42の際のセキュリティモジュール23は、乱数 R_A 、乱数 R_B 、値 V_A 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列にデジタル署名を行い Sig_A を得る。セキュリティモジュール23は、これらに証明書 $Cert_A$ を付け、メモリ記録再生装置200に送る。なお、セキュリティモジュール23がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして0を用いる。

【0325】

これら $Cert_A$, R_A , R_B , V_A , $RegV_A$, Sig_A を受け取ったメモリ記録再生装置 200 は、証明書 $Cert_A$ 、デジタル署名 Sig_A 、 ID_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 23 から返送されてきた乱数 R_B と先に生成したもののが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、自己が保持するレジストレーションリストを用い、メモリ情報記録媒体 20 の ID_A が当該レジストレーションリストに登録されていることを検証する。この検証の結果、メモリ情報記録媒体 20 の ID_A がレジストレーションリストに登録されていない場合には、当該メモリ情報記録媒体 20 は不正な媒体であると判定し、当該プロトコルを終了する。

【0326】

一方、上記 ID_A が当該レジストレーションリストに登録されており、そのメモリ情報記録媒体 20 が正当であると判断した場合、メモリ記録再生装置 200 は、手順 P43 として、 K_B の生成と $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、当該装置 200 のレジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って Sig_B を得る。メモリ記録再生装置 200 は、これらに証明書 $Cert_B$ を付け、セキュリティモジュール 23 に送る。なお、メモリ記録再生装置 200 がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして 0 を用いる。

【0327】

上記メモリ記録再生装置 200 から $Cert_B$, R_B , R_A , V_B , $RegV_B$, Sig_B を受け取ると、セキュリティモジュール 23 は、証明書 $Cert_B$ 、デジタル署名 Sig_B 、 ID_B の検証を行い、その検証をパスした時、自己が保持するレジストレーションリストを用い、メモリ記録再生装置 200 の ID_B が当該レジストレーションリストに登録されていることを検証する。この検証の結果、メモリ記録再生装置 200 の ID_B がレジストレーションリストに登録されていない場合には、当該メモリ記録再生装置 200 は不正な装置であると判定し、当該プロトコルを終了する。

【0328】

一方、メモリ記録再生装置200のID_Bが当該レジストレーションリストに登録されており、そのメモリ記録再生装置200が正当であると判断した場合、すなわち、セキュリティモジュール23とメモリ記録再生装置200の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール23とメモリ記録再生装置200はセッション鍵K_{se}を生成して共有する。

【0329】

次に、セキュリティモジュール23とメモリ記録再生装置200は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順P44又はP45として、その新しいバージョンのレジストレーションリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのレジストレーションリストが送られてきた方は、当該レジストレーションリスト内に含まれるセンタTCの署名TCSigを検証し、その検証をパスしたとき、その新しいレジストレーションリストを用いて自己が保持している古いレジストレーションリストを更新（リストのアップデート）する。

【0330】

その後の手順P46以降は、前記図20の場合と同様である。

【0331】

なお、上記レジストレーションリストの伝送は、コンテンツデータの伝送の間、または終了後に行ってもよい。

【0332】

図36には、前記第2の実施の形態における図21の手順を、レジストレーションリストにも適用した例を示している。すなわち、図36は、先にレジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のレジストレーションリストを用いて相手方のIDを検証するようにした場合の、データ再生時の手順を示している。

【0333】

この図36において、手順P52の際のセキュリティモジュール23は、乱数

R_A 、乱数 R_B 、値 V_A 、バージョンナンバー $RegV_A$ からなるビット列にデジタル署名を行って Sig_A を得、これらに証明書 $Cert_A$ を付けてメモリ記録再生装置 200 に送る。

【0334】

それらを受け取ったメモリ記録再生装置 200 は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 23 から返送されてきた乱数 R_B と先に生成したものとが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順 P53 として、 K_B を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、当該装置 200 が持つレジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って Sig_B を得る。メモリ記録再生装置 200 は、これらに証明書 $Cert_B$ を付け、セキュリティモジュール 23 に送る。

【0335】

上記メモリ記録再生装置 200 から $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RegV_B$ 、 Sig_B を受け取ると、セキュリティモジュール 23 は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行い、その検証をパスした時、次の処理に進む。

【0336】

セキュリティモジュール 23 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 23 とメモリ記録再生装置 200 は、セッション鍵 K_{se} を生成して共有する。また、セキュリティモジュール 23 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 23 とメモリ記録再生装置 200 は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行う。

【0337】

両者のバージョンナンバーが同じである場合、メモリ記録再生装置 200 とセキュリティモジュール 23 は、それぞれが保持するレジストレーションリストを用いて相手方の ID の検証を行い、互いに相手方の ID がレジストレーションリストに登録されていることを検証する。このレジストレーションリストの相互検

証の結果、両者において共にレジストレーションリストに登録されていると判定された場合には、後段の手順P56の処理に進む。また、セキュリティモジュール23において、メモリ記録再生装置200のID_Bが自己のレジストレーションリストに登録されていない場合には、当該メモリ記録再生装置200は不正な装置であると判定し、当該プロトコルを終了する。同じく、メモリ記録再生装置200において、セキュリティモジュール23のID_Aが自己のレジストレーションリストに登録されていない場合には、当該セキュリティモジュール23は不正な媒体のものであると判定し、当該プロトコルを終了する。

【0338】

一方、セキュリティモジュール23とメモリ記録再生装置200においてそれぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順P54又はP55として、上記新しいバージョンのレジストレーションリストを相手方に送り、この新しいバージョンのレジストレーションリストを受け取った側では当該新しいバージョンのレジストレーションリストを用いて相手方のID検証を行うと共に、古いバージョンのレジストレーションリストを更新する。

【0339】

その後の手順P56以降は、前記図21の場合と同様である。

【0340】

次に、この第4の実施の形態において、メモリ情報記録媒体20のメモリ部22からのデータの再生処理については、前述の図22と同様の図37に示すような手順とすることも可能である。

【0341】

この図37において、メモリ記録再生装置200とセキュリティモジュール23は、手順P62にて相互にレジストレーションリストのバージョンナンバーを交換する。

【0342】

また、手順P63、P64では、レジストレーションリストのバージョンナン

バーが古い方を、新しいバージョンナンバーのレジストレーションリストにて更新する。

【0 3 4 3】

手順 P 6 5 以降の処理は、前記図 2 2 と同様である。

【0 3 4 4】

上述した第 1 及び第 2 の実施の形態ではリボケーションリストを、第 3 及び第 4 の実施の形態ではレジストレーションリストを用いて、不正に情報が複製等されることを防止した例を挙げたが、本発明では、これらリボケーションリストとレジストレーションリストを用いることで、さらに確実に不正な情報複製等を防止することも可能である。

【0 3 4 5】

ここで、リボケーションリストとレジストレーションリストを用いる場合、それら両者を同時に用いることも可能であり、或いは、それらのうち何れか一方を優先的に使用し、他方を使用しないようにすることも可能である。特に、上記何れか一方を優先的に使用する場合は、不正者リストであるリボケーションリストを優先することが望ましい。

【0 3 4 6】

また、両者を同時に用いる場合、それらリストを区別するために、例えば図 3 8 に示すようなリストフォーマットを用いることが可能である。すなわち、この図 3 8 のリストフォーマットは、リボケーションリストとレジストレーションリストの区別と、それらのバージョンナンバーと、秘密鍵が露呈してしまった情報記録媒体或いは記録再生装置の ID（リボークされる機器又は媒体の ID）のリスト、正当な情報記録媒体或いは記録再生装置の ID（登録された機器又は媒体の ID）のリストと、センタ TC によるデジタル署名とからなるものである。

【0 3 4 7】

以下、上記リボケーションリストとレジストレーションリストを使用した第 5 の実施の形態について説明する。

【0 3 4 8】

第 5 の実施の形態は、前述の第 1、第 3 の実施の形態で説明した光ディスク情

報記録媒体 1 0 のセキュリティモジュール 1 3 の不揮発性メモリ 3 4 と、光ディスク記録再生装置 1 0 0 の不揮発性メモリ 1 1 0 に、前記リボケーションリストとレジストレーションリストを格納するようにした例である。当該第 5 の実施の形態における光ディスク情報記録媒体 1 0、光ディスク記録再生装置 1 0 0 の構成は、前記図 1 ～図 3 と同じであるため、それら構成についての説明は省略する。

【 0 3 4 9 】

図 3 9 から図 4 1 を用いて、第 5 の実施の形態の光ディスク記録再生装置 1 0 0 が光ディスク情報記録媒体 1 0 にデータを記録する手順を説明する。なお、図 3 9 ～図 4 1 は、前記第 1 の実施の形態の図 6 ～図 8、第 3 の実施の形態の図 2 4 ～図 2 6 と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、それらとは異なる部分のみ説明する。

【 0 3 5 0 】

図 3 9 は前記図 6、図 2 4 と略々同様な手順を表しており、手順 R 2 として、光ディスク記録再生装置 1 0 0 とセキュリティモジュール 1 3 との間でリボケーションリスト／レジストレーションリスト（以下、適宜、リストと呼ぶ）のバージョンナンバーを交換する。

【 0 3 5 1 】

また、手順 R 3、R 4 では、何れかの一方が他方のリボケーションリスト／レジストレーションリストより新しいリストを持っていた場合、当該新しいリストを持っている方は自分のリストを他方に送る。一方、古いリストを持っている方は、新しいリストを持っている方から、当該新しいリストを送ってもらい、その正当性を検証した後、自分が持つリストを、その送られてきた新しいリストに更新する。

【 0 3 5 2 】

なお、手順 R 3、R 4 におけるリストの送付は、後の手順 R 5 におけるデータの記録と順序が前後してもかまわない。つまり、手順 R 5 にてデータの記録を行った後に、手順 R 3 或いは R 4 でのリストの送付を行うようにしてもよい。

【0 3 5 3】

次に、図 4 0 には、上記図 3 9 に示した第 5 の実施の形態の光ディスク記録再生装置 1 0 0 が光ディスク情報記録媒体 1 0 にデータを記録するまでの手順の詳細を示しており、前記図 7、図 2 5 と略々同様な手順となっている。

【0 3 5 4】

この図 4 0 において、手順 R 1 2 の際のセキュリティモジュール 1 3 は、乱数 R_A 、乱数 R_B 、値 V_A 、リボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列 $R_A || R_B || V_A || RevV_A || RegV_A$ にデジタル署名の関数 $Sign$ を用いたデジタル署名を行い $Sig_A = Sign(PriKey_A, R_A || R_B || V_A || RevV_A || RegV_A)$ を得る。セキュリティモジュール 1 3 は、これら R_A 、 R_B 、 V_A 、 $RevV_A$ 、 $RegV_A$ 、 Sig_A に証明書 $Cert_A$ を付け、光ディスク記録再生装置 1 0 0 に送る。なお、セキュリティモジュール 1 3 がリボケーションリスト／レジストレーションリストを持たない場合或いは使用しない場合は、それぞれバージョンナンバーとして 0 を用いる。

【0 3 5 5】

これら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RevV_A$ 、 $RegV_A$ 、 Sig_A を受け取った光ディスク記録再生装置 1 0 0 は、証明書 $Cert_A$ 、デジタル署名 Sig_A 、 ID_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 1 3 から返送されてきた乱数 R_B と先に生成したもののが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、自己の不揮発性メモリ 1 1 0 に格納しているリボケーションリスト／レジストレーションリストを用い、光ディスク情報記録媒体 1 0 の ID_A が当該リストに載っているか否かを検証する。このときの検証は、上述したように両者のリストを用いても良いし、また、優先的に一方のリスト（特にリボケーションリスト）を用いても良い。この検証の結果、当該光ディスク情報記録媒体 1 0 が不正な媒体であると判定した場合は、当該プロトコルを終了する。

【0 3 5 6】

一方、上記リストを用いた検証の結果、その光ディスク情報記録媒体 1 0 が正当であると判断した場合、光ディスク記録再生装置 1 0 0 は、手順 R 1 3 として、 K_B を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値

V_B 、当該装置 1 0 0 が持つリボケーションリストのバージョンナンバー $RevV_B$ 、レジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列 $R_B || R_A || V_B || RevV_B || RegV_B$ にデジタル署名を行って $Sig_B = \text{Sign}(\text{PriKey}_B, R_B || R_A || V_B || RevV_B || RegV_B)$ を得る。光ディスク記録再生装置 1 0 0 は、これら R_B 、 R_A 、 V_B 、 $RevV_B$ 、 $RegV_B$ 、 Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール 1 3 に送る。なお、光ディスク記録再生装置 1 0 0 がリボケーションリスト／レジストレーションリストを持たない場合或いは使用しない場合は、それぞれバージョンナンバーとして 0 を用いる。

【0 3 5 7】

上記光ディスク記録再生装置 1 0 0 から $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RevV_B$ 、 $RegV_B$ 、 Sig_B を受け取ると、セキュリティモジュール 1 3 は、証明書 $Cert_B$ 、デジタル署名 Sig_B 、 ID_B の検証を行い、その検証をパスした時、自己の不揮発性メモリ 3 4 に格納しているリボケーションリスト／レジストレーションリストを用い、光ディスク記録再生装置 1 0 0 の ID_B が当該リストに載っているか否かを検証する。このときの検証は、上述したように両者のリストを用いても良いし、また、優先的に一方のリスト（特にリボケーションリスト）を用いても良い。この検証の結果、当該光ディスク記録再生装置 1 0 0 が不正な媒体であると判定した場合は、当該プロトコルを終了する。

【0 3 5 8】

一方、上記検証の結果、その光ディスク記録再生装置 1 0 0 が正当であると判断した場合、すなわち、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 はセッション鍵 K_{se} を生成して共有する。

【0 3 5 9】

次に、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 は、それぞれ相手方が持っているリボケーションリスト／レジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順 R 1 4 又は R 1 5 として、その新しいバージョンのリストを相手方

に送る。上述のように、相手方から新しいバージョンナンバーのリストが送られてきた方は、当該リスト内に含まれるセンタTCの署名TCSigを検証し、その検証をパスしたとき、その新しいリストを用いて自己が保持している古いリストを更新（リストのアップデート）する。

【0360】

その後の手順R16以降は、前記図7、図25の場合と同様である。

【0361】

なお、上記リボケーションリスト／レジストレーションリストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

【0362】

図4-1には、前記第1の実施の形態における図8や、第3の実施の形態における図26の手順を、本実施の形態のリボケーションリスト／レジストレーションリストにも適用した例を示している。すなわち、図4-1は、先にリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリストを用いて相手方のIDを検証するようにした場合の、データ記録時の手順を示している。

【0363】

この図4-1において、手順R22の際のセキュリティモジュール13は、乱数 R_A 、乱数 R_B 、値 V_A 、リボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列 $R_A || R_B || V_A || RevV_A || RegV_A$ にデジタル署名を行って Sig_A を得、これら R_A 、 R_B 、 V_A 、 $RevV_A$ 、 $RegV_A$ 、 Sig_A に証明書 $Cert_A$ を付けて光ディスク記録再生装置100に送る。

【0364】

これら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RevV_A$ 、 $RegV_A$ 、 Sig_A を受け取った光ディスク記録再生装置100は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール13から返送されてきた乱数 R_B と先に生成したものとが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順R23として、 K_B を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、当該装置100が持つリボケーションリ

ストのバージョンナンバー $RevV_B$ 、レジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って Sig_B を得る。光ディスク記録再生装置 100 は、これら R_B 、 R_A 、 V_B 、 $RevV_B$ 、 $RegV_B$ 、 Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール 13 に送る。

【0365】

上記光ディスク記録再生装置 100 から $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RevV_B$ 、 $RegV_B$ 、 Sig_B を受け取ると、セキュリティモジュール 13 は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行い、その検証をパスした時、次の処理に進む。

【0366】

上述のように、セキュリティモジュール 13 と光ディスク記録再生装置 100 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 13 と光ディスク記録再生装置 100 は、セッション鍵 K_{se} を生成して共有する。

【0367】

また、セキュリティモジュール 13 と光ディスク記録再生装置 100 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 13 と光ディスク記録再生装置 100 は、それぞれ相手方が持っているリストのバージョンナンバーのチェックを行う。

【0368】

ここで、両者のバージョンナンバーが同じである場合、光ディスク記録再生装置 100 とセキュリティモジュール 13 は、それぞれが保持するリストを用いて相手方の ID の検証を行い、互いに相手方が正当であるか否か検証する。このときの検証は、上述したように両者のリストを用いても良いし、また、優先的に一方のリスト（特にリボケーションリスト）を用いても良い。この検証の結果、両者が共に正当であると判定された場合には、後段の手順 R26 の処理に進む。また、セキュリティモジュール 13 において、光ディスク記録再生装置 100 が不正な装置であると判定した場合は、当該プロトコルを終了する。同じく、光ディスク記録再生装置 100 において、セキュリティモジュール 13 が不正な媒体のものであると判定した場合は、当該プロトコルを終了する。

【0 3 6 9】

一方、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 においてそれぞれ相手方が持っているリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順 R 2 4 又は R 2 5 として、上記新しいバージョンのリストを相手方に送り、この新しいバージョンのリストを受け取った側では当該新しいバージョンのリストを用いて相手方の I D 検証を行うと共に、古いバージョンのリストを更新する。

【0 3 7 0】

その後の手順 R 2 6 以降は、前記図 8、図 2 6 の場合と同様である。

【0 3 7 1】

次に、図 4 2 ～図 4 4 を用いて、上記第 5 の実施の形態の光ディスク記録再生装置 1 0 0 が光ディスク 1 2 からデータを再生する手順を説明する。なお、図 4 2 ～図 4 4 は、前記第 1 の実施の形態の図 9 ～図 1 1、第 3 の実施の形態の図 2 7 ～図 2 9 と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図 9 ～図 1 1、図 2 7 ～図 2 9 とは異なる部分のみ説明する。

【0 3 7 2】

図 4 2 において、光ディスク記録再生装置 1 0 0 とセキュリティモジュール 1 3 は、手順 P 2 にて、リボケーションリスト／レジストレーションリストを用い、互いに相手方が正当なものであることの確認を行い、自分が持つリストのバージョンナンバーを送り合う。

【0 3 7 3】

また、手順 P 3、P 4 として、光ディスク記録再生装置 1 0 0 とセキュリティモジュール 1 3 は、どちらかが相対的に新しいリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のリストを更新することも同様である。

【0 3 7 4】

その後の手順 P 5 以降は、前記図 9、図 2 7 の場合と同様である。

【0375】

次に、図43には、上記図42に示した第5の実施の形態の光ディスク記録再生装置100が光ディスク情報記録媒体10からデータを再生するまでの手順の詳細を示している。なお、当該図43の手順は、前記図10、図28と略々同様な手順となっている。

【0376】

この図43において、手順P12の際のセキュリティモジュール13は、乱数 R_A 、乱数 R_B 、値 V_A 、リボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列にデジタル署名を行い Sig_A を得る。セキュリティモジュール13は、これらに証明書 $Cert_A$ を付け、光ディスク記録再生装置100に送る。なお、セキュリティモジュール13がリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして0を用いる。

【0377】

これら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RevV_A$ 、 $RegV_A$ 、 Sig_A を受け取った光ディスク記録再生装置100は、証明書 $Cert_A$ 、デジタル署名 Sig_A 、 ID_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール13から返送されてきた乱数 R_B と先に生成したものとが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、自己の不揮発性メモリ110に格納しているリストを用い、光ディスク情報記録媒体10の ID_A が正当であるか否かを検証する。この検証の結果、光ディスク情報記録媒体10の ID_A が不正な媒体であると判定された場合は、当該プロトコルを終了する。

【0378】

一方、光ディスク情報記録媒体10が正当であると判断した場合、光ディスク記録再生装置100は、手順P13として、 K_B を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、当該装置100のリボケーションリストのバージョンナンバー $RevV_B$ 、レジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って Sig_B を得る。光ディスク記録再生装置100は、これら R_B 、 R_A 、 V_B 、 $RegV_B$ 、 $RevV_B$ 、 Sig

B に証明書 $Cert_B$ を付け、セキュリティモジュール 1 3 に送る。なお、光ディスク記録再生装置 1 0 0 がリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして 0 を用いる。

【0 3 7 9】

上記光ディスク記録再生装置 1 0 0 から $Cert_B$, R_B , R_A , V_B , $RevV_B$, $RegV_B$, Sig_B を受け取ると、セキュリティモジュール 1 3 は、証明書 $Cert_B$ 、デジタル署名 Sig_B 、 ID_B の検証を行い、その検証をパスした時、自己の不揮発性メモリ 3 4 に格納しているリストを用い、光ディスク記録再生装置 1 0 0 が正当であるか否か検証する。この検証の結果、光ディスク記録再生装置 1 0 0 が不正な装置であると判定した場合は、当該プロトコルを終了する。

【0 3 8 0】

一方、光ディスク記録再生装置 1 0 0 が正当であると判断した場合、すなわち、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 はセッション鍵 K_{se} を生成して共有する。

【0 3 8 1】

次に、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 は、それぞれ相手方が持っているリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順 P 1 4 又は P 1 5 として、その新しいバージョンのリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのリストが送られてきた方は、当該リスト内に含まれるセンタ TC の署名 TC_{Sig} を検証し、その検証をパスしたとき、その新しいリストを用いて自己が保持している古いリストを更新（リストのアップデート）する。

【0 3 8 2】

その後の手順 P 1 6 以降は、前記図 1 0、図 2 8 の場合と同様である。

【0 3 8 3】

なお、上記リストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

【0384】

図44には、前記第1の実施の形態における図11の手順、第3の実施の形態における図29の手順を、リボケーションリスト/レジストレーションリストにも適用した例を示している。すなわち、図44は、先にリボケーションリスト/レジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリストを用いて相手方のIDを検証するようにした場合の、データ再生時の手順を示している。

【0385】

この図44において、手順P22の際のセキュリティモジュール13は、乱数 R_A 、乱数 R_B 、値 V_A 、リボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列にデジタル署名を行って Sig_A を得、これらに証明書 $Cert_A$ を付けて光ディスク記録再生装置100に送る。

【0386】

それらを受け取った光ディスク記録再生装置100は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール13から返送されてきた乱数 R_B と先に生成したものとが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順P23として、 K_B を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、当該装置100が持つリボケーションリストのバージョンナンバー $RevV_B$ 、レジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って Sig_B を得る。光ディスク記録再生装置100は、これら R_B 、 R_A 、 V_B 、 $RegV_B$ 、 Sig_B に証明書 $Cert_B$ を付け、セキュリティ 上記光ディスク記録再生装置100から $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RevV_B$ 、 $RegV_B$ 、 Sig_B を受け取ると、セキュリティモジュール13は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行い、その検証をパスした時、次の処理に進む。

【0387】

セキュリティモジュール13と光ディスク記録再生装置100の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール13と光

ディスク記録再生装置 1 0 0 は、セッション鍵 K_{se}を生成して共有する。また、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 は、それぞれ相手方が持っているリストのバージョンナンバーのチェックを行う。

【0 3 8 8】

両者のバージョンナンバーが同じである場合、光ディスク記録再生装置 1 0 0 とセキュリティモジュール 1 3 は、それぞれが保持するリストを用いて相手方の I D の検証を行い、互いに相手方が正当であるか否かを検証する。このリストの相互検証の結果、両者において共に正当であると判定された場合には、後段の手順 P 2 6 の処理に進む。~~また、セキュリティモジュール 1 3 において、光ディスク記録再生装置 1 0 0 が不正な装置であると判定した場合は、当該プロトコルを終了する。同じく、光ディスク記録再生装置 1 0 0 において、セキュリティモジュール 1 3 が不正な媒体のものであると判定した場合は、当該プロトコルを終了する。~~

【0 3 8 9】

一方、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 においてそれぞれ相手方が持っているリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順 P 2 4 又は P 2 5 として、上記新しいバージョンのリストを相手方に送り、この新しいバージョンのリストを受け取った側では当該新しいバージョンのリストを用いて相手方の I D 検証を行うと共に、古いバージョンのリストを更新する。

【0 3 9 0】

その後の手順 P 2 6 以降は、前記図 1 1、図 2 9 の場合と同様である。

【0 3 9 1】

次に、本発明の第 6 の実施の形態について説明する。

【0 3 9 2】

第 6 の実施の形態は、前述の第 2、第 4 の実施の形態で説明したメモリ情報記

録媒体 2 0 のセキュリティモジュール 2 3 の不揮発性メモリ 4 4 と、メモリ記録再生装置 2 0 0 の不揮発性メモリ 2 1 0 に、前記リボケーションリストとレジストレーションリストを格納するようにした例である。当該第 6 の実施の形態におけるメモリ情報記録媒体 2 0、メモリ記録再生装置 2 0 0 の構成は、前記図 1 2 ～図 1 4 と同じであるため、それら構成についての説明は省略する。

【0393】

図 4 5 ～図 4 8 を用いて、第 6 の実施の形態のメモリ記録再生装置 2 0 0 がメモリ情報記録媒体 2 0 にデータを記録する手順を説明する。なお、図 4 5 ～図 4 8 は、前記第 2 の実施の形態の図 1 5 ～図 1 8、第 4 の実施の形態の図 3 0 ～図 3 3 と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図 1 5 ～図 1 8、図 3 0 ～図 3 3 とは異なる部分のみ説明する。

【0394】

図 4 5 は前記図 1 5、図 3 0 と略々同様な手順を表しており、手順 R 3 2 として、メモリ記録再生装置 2 0 0 とセキュリティモジュール 2 3 との間でリボケーションリスト／レジストレーションリストのバージョンナンバーを交換する。

【0395】

また、手順 R 3 3、R 3 4 では、何れかの一方が他方のリストより新しいリストを持っていた場合、当該新しいリストを持っている方は自分のリストを他方に送る。一方、古いリストを持っている方は、新しいリストを持っている方から、当該新しいリストを送ってもらい、その正当性を検証した後、自分が持つリストを、その送られてきた新しいリストに更新する。

【0396】

なお、手順 R 3 3、R 3 4 におけるリストの送付は、後の手順 R 5 におけるデータの記録と順序が前後してもかまわない。つまり、手順 R 3 5 にてデータの記録を行った後に、手順 R 3 3 或いは R 3 4 でのリストの送付を行うようにしてもよい。

【0397】

次に、図 4 6 には、上記図 4 5 に示した第 6 の実施の形態のメモリ記録再生装置 2 0 0 がメモリ情報記録媒体 2 0 にデータを記録するまでの手順の詳細を示し

ており、前記図 1 6、図 3 1 と略々同様な手順となっている。

【0 3 9 8】

この図 4 6 において、手順 R 4 2 の際のセキュリティモジュール 2 3 は、乱数 R_A 、乱数 R_B 、値 V_A 、リボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列にデジタル署名を行い Sig_A を得る。セキュリティモジュール 2 3 は、これらに証明書 $Cert_A$ を付け、メモリ記録再生装置 2 0 0 に送る。なお、セキュリティモジュール 2 3 がリボケーションリスト／レジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして 0 を用いる。

【0 3 9 9】

それら $Cert_A$, R_A , R_B , V_A , $RevV_A$, $RegV_A$, Sig_A を受け取ったメモリ記録再生装置 2 0 0 は、証明書 $Cert_A$ 、デジタル署名 Sig_A 、 ID_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 2 3 から返送されてきた乱数 R_B と先に生成したもののが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、自己が保持しているリボケーションリスト／レジストレーションリストを用い、メモリ情報記録媒体 2 0 が正当なものであるか否か検証する。この検証の結果、メモリ情報記録媒体 2 0 が不正な媒体であると判定された場合は、当該プロトコルを終了する。

【0 4 0 0】

一方、上記メモリ情報記録媒体 2 0 が正当であると判断された場合、メモリ記録再生装置 2 0 0 は、手順 R 4 3 として、 K_B の生成と $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、当該装置 2 0 0 が持つリボケーションリストのバージョンナンバー $RevV_B$ 、レジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って Sig_B を得る。メモリ記録再生装置 2 0 0 は、これらに証明書 $Cert_B$ を付け、セキュリティモジュール 2 3 に送る。なお、メモリ記録再生装置 2 0 0 がリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして 0 を用いる。

【0 4 0 1】

上記メモリ記録再生装置 2 0 0 から $Cert_B$, R_B , R_A , V_B , $RevV_B$, $RegV$

B 、 Sig_B を受け取ると、セキュリティモジュール23は、証明書 $Cert_B$ 、デジタル署名 Sig_B 、 ID_B の検証を行い、その検証をパスした時、自己が保持するリボケーションリスト／レジストレーションリストを用い、メモリ記録再生装置200が正当であるか否か検証する。この検証の結果、メモリ記録再生装置200が不正な装置であると判定された場合は、当該プロトコルを終了する。

【0402】

一方、メモリ記録再生装置200が正当であると判断された場合、すなわち、セキュリティモジュール23とメモリ記録再生装置200の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール23とメモリ記録再生装置200はセッション鍵 K_{se} を生成して共有する。

【0403】

次に、セキュリティモジュール23とメモリ記録再生装置200は、それぞれ相手方が持っているリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順R44又はR45として、その新しいバージョンのリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのリストが送られてきた方は、当該リスト内に含まれるセンタTCの署名 TC_{Sig} を検証し、その検証をパスしたとき、その新しいリストを用いて自己が保持している古いリストを更新（リストのアップデート）する。

【0404】

その後の手順R46以降は、前記図16、図31の場合と同様である。

【0405】

なお、上記リストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

【0406】

図47には、前記第2の実施の形態における図17の手順、第4の実施の形態における図32の手順を、リボケーションリスト／レジストレーションリストにも適用した例を示している。すなわち、図47では、先にリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリストを用いて相手方のIDを検証するようにした場合の、データ記録時の手順を示している。

【0407】

この図47において、手順R52の際のセキュリティモジュール23は、乱数 R_A 、乱数 R_B 、値 V_A 、リボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列にデジタル署名を行って Sig_A を得、これらに証明書 $Cert_A$ を付けてメモリ記録再生装置200に送る。

【0408】

これら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RevV_A$ 、 $RegV_A$ 、 Sig_A を受け取ったメモリ記録再生装置200は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール23から返送されてきた乱数 R_B と先に生成したものとが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順R53として、 K_B を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、当該装置200が持つリボケーションリストのバージョンナンバー $RevV_B$ 、レジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って Sig_B を得る。メモリ記録再生装置200は、これら R_B 、 R_A 、 V_B 、 $RegV_B$ 、 $RevV_B$ 、 Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール23に送る。

【0409】

上記メモリ記録再生装置200から $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RevV_B$ 、 $RegV_B$ 、 Sig_B を受け取ると、セキュリティモジュール23は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行い、その検証をパスした時、次の処理に進む。

【0410】

上述のように、セキュリティモジュール23とメモリ記録再生装置200の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール23とメモリ記録再生装置200は、セッション鍵 K_{se} を生成して共有する。

【0411】

また、セキュリティモジュール23とメモリ記録再生装置200の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール23とメモリ記録再生装置200は、それぞれ相手方が持っているリストのバージョン

ナンバーのチェックを行う。

【0412】

ここで、両者のバージョンナンバーが同じである場合、メモリ記録再生装置200とセキュリティモジュール23は、それぞれが保持するリストを用いて相手方のIDの検証を行い、互いに相手方のIDがリストに登録されていることを検証する。このリストの相互検証の結果、両者において共にリストに登録されていると判定された場合には、後段の手順R56の処理に進む。また、セキュリティモジュール23において、メモリ記録再生装置200が不正な装置であると判定された場合は、当該プロトコルを終了する。同じく、メモリ記録再生装置200において、セキュリティモジュール23が不正な媒体のものであると判定された場合は、当該プロトコルを終了する。

【0413】

一方、セキュリティモジュール23とメモリ記録再生装置200においてそれぞれ相手方が持っているリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順R54又はR55として、上記新しいバージョンのリストを相手方に送り、この新しいバージョンのリストを受け取った側では当該新しいバージョンのリストを用いて相手方のID検証を行うと共に、古いバージョンのリストを更新する。

【0414】

その後の手順R56以降は、前記図17、図32の場合と同様である。

【0415】

次に、この第6の実施の形態において、メモリ情報記録媒体20のメモリ部22へのデータの記録処理については、前述の図18や図33と同様の図48に示すような手順とすることも可能である。

【0416】

この図48において、メモリ記録再生装置200とセキュリティモジュール23は、手順R62にて相互にリボケーションリスト/レジストレーションリストのバージョンナンバーを交換する。

【 0 4 1 7 】

また、手順 R 6 3、R 6 4 では、リストのバージョンナンバーが古い方を、新しいバージョンナンバーのリストにて更新する。

【 0 4 1 8 】

手順 R 6 5 以降の処理は、前記図 1 8、図 3 3 と同様である。

【 0 4 1 9 】

次に、図 4 9 ～ 図 5 2 を用いて、上記第 6 の実施の形態のメモリ記録再生装置 2 0 0 がメモリ情報記録媒体 2 0 のメモリ部 2 2 からデータを再生する手順を説明する。なお、図 4 9 ～ 図 5 2 は、前記第 2 の実施の形態の図 1 9 ～ 図 2 2 や第 4 の実施の形態の図 3 4 ～ 図 3 7 と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図 1 9 ～ 図 2 2 や図 3 4 ～ 図 3 7 とは異なる部分のみ説明する。

【 0 4 2 0 】

図 4 9 において、メモリ記録再生装置 2 0 0 とセキュリティモジュール 2 3 は、手順 P 3 2 にて、リボケーションリスト／レジストレーションリストに相手方の ID が載せられていないことの確認を互いに行い、自分が持つリストのバージョンナンバーを送り合う。

【 0 4 2 1 】

また、手順 P 3 3、P 3 4 として、メモリ記録再生装置 2 0 0 とセキュリティモジュール 2 3 は、どちらかが相対的に新しいリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のリストを更新することも同様である。

【 0 4 2 2 】

その後の手順 P 3 5 以降は、前記図 1 9、図 3 4 の場合と同様である。

【 0 4 2 3 】

次に、図 5 0 には、上記図 2 0 に示した第 2 の実施の形態や図 3 5 に示した第 4 の実施の形態のメモリ記録再生装置 2 0 0 がメモリ部 2 2 からデータを再生するまでの手順の詳細を示している。なお、当該図 5 0 の手順は、前記図 2 0、図 3 5 と略々同様な手順となっている。

【0424】

この図50において、手順P42の際のセキュリティモジュール23は、乱数 R_A 、乱数 R_B 、値 V_A 、リボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列にデジタル署名を行い Sig_A を得る。セキュリティモジュール23は、これらに証明書 $Cert_A$ を付け、メモリ記録再生装置200に送る。なお、セキュリティモジュール23がリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして0を用いる。

【0425】

これら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RevV_A$ 、 $RegV_A$ 、 Sig_A を受け取ったメモリ記録再生装置200は、証明書 $Cert_A$ 、デジタル署名 Sig_A 、 ID_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール23から返送されてきた乱数 R_B と先に生成したものが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、自己が保持するリストを用い、メモリ情報記録媒体20が正当であるか否かの検証を行う。この検証の結果、メモリ情報記録媒体20が不正な媒体であると判定した場合は、当該プロトコルを終了する。

【0426】

一方、上記メモリ情報記録媒体20が正当であると判断した場合、メモリ記録再生装置200は、手順P43として、 K_B の生成と $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、当該装置200のレジストレーションリストのバージョンナンバー $RevV_B$ 、レジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って Sig_B を得る。メモリ記録再生装置200は、これらに証明書 $Cert_B$ を付け、セキュリティモジュール23に送る。なお、メモリ記録再生装置200がリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして0を用いる。

【0427】

上記メモリ記録再生装置200から $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RevV_B$ 、 $RegV_B$ 、 Sig_B を受け取ると、セキュリティモジュール23は、証明書 $Cert_B$ 、デジタル署名 Sig_B 、 ID_B の検証を行い、その検証をパスした時、自己が保持するリス

トを用い、メモリ記録再生装置 200 が正当であるか否かを検証する。この検証の結果、メモリ記録再生装置 200 が不正な装置であると判定した場合は、当該プロトコルを終了する。

【0428】

一方、メモリ記録再生装置 200 が正当であると判断した場合、すなわち、セキュリティモジュール 23 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 23 とメモリ記録再生装置 200 はセッション鍵 K_{se}を生成して共有する。

【0429】

次に、セキュリティモジュール 23 とメモリ記録再生装置 200 は、それぞれ相手方が持っているリボケーションリスト／レジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順 P44 又は P45 として、その新しいバージョンのリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのリストが送られてきた方は、当該リスト内に含まれるセンタ TC の署名 TC Sig を検証し、その検証をパスしたとき、その新しいリストを用いて自己が保持している古いリストを更新する。

【0430】

その後の手順 P46 以降は、前記図 20、図 35 の場合と同様である。

【0431】

なお、上記リストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

【0432】

図 51 には、前記第 2 の実施の形態における図 21 や第 4 の実施の形態における図 36 の手順を、リボケーションリスト／レジストレーションリストにも適用した例を示している。すなわち、図 51 は、先にリボケーションリスト／レジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリストを用いて相手方の ID を検証するようにした場合の、データ再生時の手順を示している。

【0 4 3 3】

この図 5 1 において、手順 P 5 2 の際のセキュリティモジュール 2 3 は、乱数 R_A 、乱数 R_B 、値 V_A 、リボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストバージョンナンバー $RegV_A$ からなるビット列にデジタル署名を行って Sig_A を得、これらに証明書 $Cert_A$ を付けてメモリ記録再生装置 2 0 0 に送る。

【0 4 3 4】

それらを受け取ったメモリ記録再生装置 2 0 0 は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 2 3 から返送されてきた乱数 R_B と先に生成したものとが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順 P 5 3 として、 K_B を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 R_B 、乱数 R_A 、値 V_B 、当該装置 2 0 0 が持つリボケーションリストのバージョンナンバー $RevV_B$ 、レジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って Sig_B を得る。メモリ記録再生装置 2 0 0 は、これらに証明書 $Cert_B$ を付け、セキュリティモジュール 2 3 に送る。

【0 4 3 5】

上記メモリ記録再生装置 2 0 0 から $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RevV_B$ 、 $RegV_B$ 、 Sig_B を受け取ると、セキュリティモジュール 2 3 は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行い、その検証をパスした時、次の処理に進む。

【0 4 3 6】

セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 は、セッション鍵 K_{se} を生成して共有する。また、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 は、それぞれ相手方が持っているリストのバージョンナンバーのチェックを行う。

【 0 4 3 7 】

両者のバージョンナンバーが同じである場合、メモリ記録再生装置 2 0 0 とセキュリティモジュール 2 3 は、それぞれが保持するリストを用いて相手方の ID の検証を行い、互いに相手方が正当であるか否かの検証を行う。このリストの相互検証の結果、両者において共に正当であると判定された場合は、後段の手順 P 5 6 の処理に進む。また、セキュリティモジュール 2 3 において、メモリ記録再生装置 2 0 0 が不正な装置であると判定した場合は、当該プロトコルを終了する。同じく、メモリ記録再生装置 2 0 0 において、セキュリティモジュール 2 3 が不正な媒体のものであると判定した場合は、当該プロトコルを終了する。

【 0 4 3 8 】

一方、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 においてそれぞれ相手方が持っているリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順 P 5 4 又は P 5 5 として、上記新しいバージョンのリストを相手方に送り、この新しいバージョンのリストを受け取った側では当該新しいバージョンのリストを用いて相手方の ID 検証を行うと共に、古いバージョンのリストを更新する。

【 0 4 3 9 】

その後の手順 P 5 6 以降は、前記図 2 1、図 3 6 の場合と同様である。

【 0 4 4 0 】

次に、この第 6 の実施の形態において、メモリ情報記録媒体 2 0 のメモリ部 2 2 からのデータの再生処理については、前述の図 2 2 や図 3 7 と同様の図 5 2 に示すような手順とすることも可能である。

【 0 4 4 1 】

この図 5 2 において、メモリ記録再生装置 2 0 0 とセキュリティモジュール 2 3 は、手順 P 6 2 にて相互にリボケーションリスト／レジストレーションリストのバージョンナンバーを交換する。

【 0 4 4 2 】

また、手順 P 6 3、P 6 4 では、リストのバージョンナンバーが古い方を、新しいバージョンナンバーのリストにて更新する。

【0 4 4 3】

手順 P 6 5 以降の処理は、前記図 2 2、図 3 7 と同様である。

【0 4 4 4】

ところで、上述した第 1 ～ 第 6 の実施の形態では、記録再生装置（1 0 0、2 0 0）が不揮発性メモリ（1 1 0、2 1 0）を備え、情報記録媒体のセキュリティモジュール（1 3、2 3）が不揮発性メモリ（3 4、4 4）を備え、これら不揮発性メモリにリボケーションリスト及び／又はレジストレーションリストを格納している例について説明したが、それら記録再生装置と情報記録媒体の何れか一方或いは両方において、リボケーションリスト／レジストレーションリストを格納するための不揮発性メモリを備えていない場合も考えられる。すなわち、リストを格納するための不揮発性メモリを備えることは、コストの上昇に繋がるため、当該不揮発性メモリを備えない記録再生装置や情報記録媒体、或いは、秘密鍵や公開鍵は記憶できるがリストの情報については記憶できるだけの十分な記憶容量を持たない安価な不揮発性メモリしか備えていない記録再生装置や情報記録媒体が存在することが考えられる。

【0 4 4 5】

なお、本発明の各実施の形態では、一つの不揮発性メモリにリストを格納する例を挙げているが、もちろん 2 以上の不揮発性メモリにリストを格納しても、また一つの不揮発性メモリ内の一部の領域にリストを格納するようにしても良い。さらに、情報記録媒体内に設けられる不揮発性メモリは、セキュリティモジュールの外に配置されるものであってもよい。言い換えると、上述した各実施の形態において、リストを格納するための不揮発性メモリとは、前記暗号化されたコンテンツデータを記録する領域（前記光ディスク 1 2 のデータ記憶領域や、メモリ部 2 2）以外の記憶領域であって、上記リストを記憶するために特に設けられた記憶領域のことを意味しており、公開鍵や秘密鍵を保持する記憶領域とは異なっている。

【0 4 4 6】

ここで、リボケーションリスト及び／又はレジストレーションリストを十分に格納できる不揮発性メモリを備えるか否かにより、上記情報記録媒体は以下に説

明する第 1、第 2 の媒体タイプに分類することができ、また、上記記録再生装置は、以下の第 1、第 2 の装置タイプに分類することができる。

【0 4 4 7】

第 1 の媒体タイプは、情報記録媒体が、上記リボケーションリスト及び／又はレジストレーションリストを格納するための不揮発性メモリを備えておらず、これらリストを当該情報記録媒体のコンテンツデータ記録用の領域に格納するようにした場合である。なお、第 1 の媒体タイプには、上記不揮発性メモリが上記リストを格納するのに十分な記憶容量を有していない場合も含む。

【0 4 4 8】

第 2 の媒体タイプは、情報記録媒体が上記リボケーションリスト及び／又はレジストレーションリストを格納するための不揮発性メモリを備えている場合である。

【0 4 4 9】

第 1 の装置タイプは、記録再生装置が、上記リボケーションリスト及び／又はレジストレーションリストを格納するための不揮発性メモリを備えていない場合である。なお、第 1 の装置タイプには、上記不揮発性メモリが上記リストを格納するのに十分な記憶容量を有していない場合も含む。

【0 4 5 0】

第 2 の装置タイプは、記録再生装置が、上記リボケーションリスト及び／又はレジストレーションリストを格納するための不揮発性メモリを備えている場合である。

【0 4 5 1】

なお、以下の説明では、上記第 1 の媒体タイプに相当する光ディスク情報記録媒体をメディアタイプ IM1 とし、上記第 2 の媒体タイプに相当する光ディスク情報記録媒体をメディアタイプ IM2 とし、上記第 1 の媒体タイプに相当するメモリ情報記録媒体をメディアタイプ IM3 とし、上記第 2 の媒体タイプに相当するメモリ情報記録媒体をメディアタイプ IM4 と呼ぶことにする。さらに、上記第 1 の装置タイプに相当する光ディスク記録再生装置をデバイスタイプ Dev1 とし、上記第 2 の装置タイプに相当する光ディスク記録再生装置をデバイスタイ

プDev2とし、上記第1の装置タイプに相当するメモリ記録再生装置をデバイスタイプDev3とし、上記第2の装置タイプに相当するメモリ記録再生装置をデバイスタイプDev4とする。

【0452】

図53には、当該メディアタイプIM1に相当する光ディスク情報記録媒体50の概略構成を示す。この図53に示すメディアタイプIM1の光ディスク情報記録媒体50は、図54に示すように、リストを格納するための不揮発性メモリを持たないセキュリティモジュール53を備えている。ただし、この図54に示すようにリストを格納するための不揮発性メモリを持たないセキュリティモジュール53であっても、秘密鍵、公開鍵証明書、ID、バージョンナンバーを記憶するためのメモリは必要であり、したがって、当該図54のセキュリティモジュール53は、それら秘密鍵、公開鍵証明書、ID、バージョンナンバーを記憶するための不揮発性の鍵メモリ36を備えている。なお、図53、図54における各部の構成は、前述の図1、図2の例と同じであるため、それらの説明は省略する。

【0453】

また、図55には、上記メディアタイプIM3に相当するメモリ情報記録媒体60の概略構成を示す。この図55に示すメディアタイプIM3のメモリ情報記録媒体60は、図56に示すように、リストを格納するための不揮発性メモリを持たないセキュリティモジュール63を備えている。なお、これら図55、図56における各部の構成は前述の図11、図12の例と同じであるため、それらの説明は省略する。

【0454】

以下、上記メディアタイプIM1とデバイスタイプDev1の組み合わせ(IM1, Dev1)、メディアタイプIM1とデバイスタイプDev2の組み合わせ(IM1, Dev2)、メディアタイプIM2とデバイスタイプDev1の組み合わせ(IM2, Dev1)、メディアタイプIM3とデバイスタイプDev3の組み合わせ(IM3, Dev3)、メディアタイプIM3とデバイスタイプDev4の組み合わせ(IM3, Dev4)、メディアタイプIM4とデバイス

タイプDev 3の組み合わせ(IM4, Dev 3)のそれぞれについて、データ記録時と再生時の手順の説明を行う。なお、メディアタイプIM2とデバイスタイプDev 2との組み合わせ(IM2, Dev 2)は、前述した第1、第3、第5の実施の形態に相当し、メディアタイプIM4とデバイスタイプDev 4との組み合わせ(IM4, Dev 4)は前述した第2、第4、第6の実施の形態に相当するため、これらの組み合わせについての説明は省略する。

【0455】

なお、以下の説明では、前述した第5、第6の実施の形態のように、リストとしてリボケーションリストとレジストレーションリストの両方を利用可能とした例を挙げて説明しているが、前述の第1～第4の実施の形態のように何れか一方のリストのみ使用する場合であっても良いことは言うまでもない。また、以下の各実施の形態の説明では、先にリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリストを用いて相手方のIDを検証するようにした場合を例に挙げており、前述の第1～第6の実施の形態にて説明した全ての手順に対応する説明は行わないが、以下の各実施の形態においても前記第1～第6の実施の形態にて説明した全ての手順と同様の手順で処理を行うことは可能である。

【0456】

先ず、第7の実施の形態として、メディアタイプIM1とデバイスタイプDev 1の組み合わせ(IM1, Dev 1)から説明する。

【0457】

当該第7の実施の形態の組み合わせにおけるシステム構成は、図57に示すようになる。すなわち、デバイスタイプDev 1の光ディスク記録再生装置300はリストを格納するための専用の不揮発性メモリを備えておらず(或いはリストを記憶できる十分な記憶容量を備えていない不揮発性メモリのみ有する)、また、メディアタイプIM1の光ディスク情報記録媒体50のセキュリティモジュール53はリストを格納するための不揮発性メモリを備えていない(或いはリストを記憶できる十分な記憶容量を備えていない不揮発性メモリのみ有する)。ただし、この図57に示すようにリストを格納するための専用の不揮発性メモリを持たない光ディスク記録再生装置300であっても、秘密鍵、公開鍵証明書、ID

、バージョンナンバーを記憶するためのメモリは必要であり、したがって、当該図 5 7 の光ディスク記録再生装置 3 0 0 は、それら秘密鍵、公開鍵証明書、ID、バージョンナンバーを記憶するための不揮発性の鍵メモリ 1 1 1 を備えている。なお、当該図 5 7 における各部の構成は、前述の図 3 の例と同じであるため、それらの説明は省略する。

【0 4 5 8】

図 5 8 には、当該第 7 の実施の形態のメディアタイプ IM 1 とデバイスタイプ Dev 1 の組み合わせ (IM 1, Dev 1) の場合に、光ディスク記録再生装置 3 0 0 が光ディスク情報記録媒体 5 0 にデータを記録する手順を説明する。なお、図 5 8 において前述の各実施の形態の略々同じ手順についての説明は省略し、

以下の説明では、それらと異なる部分のみ説明する。

【0 4 5 9】

図 5 8 は前記図 3 9 と略々同様な手順を表しており、手順 R 2 として、光ディスク記録再生装置 3 0 0 とセキュリティモジュール 5 3 との間でリボケーションリスト/レジストレーションリストのバージョンナンバーを交換する。ここで、当該第 7 の実施の形態の場合は、光ディスク記録再生装置 3 0 0 はリストを持たないため、バージョンナンバー「0」をセキュリティモジュール 5 3 に送り、また、光ディスク情報記録媒体 5 0 は光ディスク 1 2 のコンテンツデータ記録用の領域に記録されているリボケーションリスト/レジストレーションリストのバージョンナンバーを光ディスク記録再生装置 3 0 0 に送ることになる。このバージョンナンバーは、光ディスク情報記録媒体 5 0 のセキュリティモジュールが覚えておく。

【0 4 6 0】

次に、光ディスク記録再生装置 3 0 0 は、手順 R 1 0 3 として、光ディスク情報記録媒体 5 0 の光ディスク 1 2 のコンテンツデータ記録用の領域に記録されているリボケーションリスト/レジストレーションリストを読み出す。

【0 4 6 1】

当該光ディスク記録再生装置 3 0 0 は、上記光ディスク情報記録媒体 5 0 から読み出したリストを用いて、当該光ディスク情報記録媒体 5 0 が正当なものである

るか否か検証し、その検証の結果、当該光ディスク情報記録媒体 5 0 が不正なものであると判定した時は、当該プロトコルを終了する。一方、その光ディスク情報記録媒体 5 0 が正当であると判定した場合は、手順 R 1 0 4 として、上記リストをセキュリティモジュール 5 3 に送る。

【 0 4 6 2 】

セキュリティモジュール 5 3 は、当該リストを用いて、光ディスク記録再生装置 3 0 0 が正当であるか否かの検証を行い、不正である場合はプロトコルを終了する。

【 0 4 6 3 】

上記セキュリティモジュール 5 3 が上記リストを用いた検証により正当であると判定した場合、すなわち、光ディスク記録再生装置 3 0 0 とセキュリティモジュール 5 3 の両者が共に正当であると判定した場合は、後段のデータ暗号化と記録の手順 R 5 に進むことになる。

【 0 4 6 4 】

次に、図 5 9 には、上記図 5 8 に示した第 7 の実施の形態の光ディスク記録再生装置 3 0 0 が光ディスク情報記録媒体 5 0 にデータを記録するまでの手順の詳細を示しており、前記図 4 0 と略々同様な手順となっている。

【 0 4 6 5 】

この図 5 9 において、セキュリティモジュール 5 3 は、手順 R 1 2 の際に、乱数 R_A 、乱数 R_B 、値 V_A 、光ディスク 1 2 のデータ記録領域に格納されているリボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列に証明書 $Cert_A$ を付け、光ディスク記録再生装置 3 0 0 に送る。なお、リボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ は、セキュリティモジュールが覚えておく。

【 0 4 6 6 】

これら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RevV_A$ 、 $RegV_A$ 、 Sig_A を受け取った光ディスク記録再生装置 3 0 0 は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 5 3 から返送されてきた乱

数 R_B と先に生成したものとが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順 R 1 3 として、乱数 R_B 、乱数 R_A 、値 V_B 、自己がリストを持たないことを示す「0」のバージョンナンバーからなるビット列にデジタル署名を行い、これら R_B 、 R_A 、 V_B 、0、0、 Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール 5 3 に送る。

【0 4 6 7】

上記光ディスク記録再生装置 3 0 0 から $Cert_B$ 、 R_B 、 R_A 、 V_B 、0、0、 Sig_B を受け取ると、セキュリティモジュール 5 3 は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

【0 4 6 8】

ここで、セキュリティモジュール 5 3 にて当該検証をパスしたとき、すなわち、光ディスク記録再生装置 3 0 0 とセキュリティモジュール 5 3 の両方で検証をパスしたとき、セキュリティモジュール 5 3 と光ディスク記録再生装置 3 0 0 はセッション鍵 K_{se} を生成して共有する。

【0 4 6 9】

次に、光ディスク記録再生装置 3 0 0 は、手順 R 1 1 4 として、光ディスク 1 2 のデータ記録領域に格納されているリボケーションリスト／レジストレーションリストを読み取り、そのリストのバージョンナンバーが先の手順 R 1 2 で取得したバージョンナンバー ($RevV_A$ 、 $RegV_A$) と等しいこと、及び、当該リストを用いて光ディスク情報記録媒体 5 0 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC の署名 $TC Sig$ の検証を行う。当該検証において、光ディスク情報記録媒体 5 0 が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、光ディスク記録再生装置 3 0 0 は、手順 R 1 1 5 として、そのリストをセキュリティモジュール 5 3 に送る。なお、セキュリティモジュール 5 3 にリストを送るのは、検証の途中であっても良い。

【0 4 7 0】

上記リストを受け取ったセキュリティモジュール 5 3 は、そのリストのバージ

ョンナンバーが前記バージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いて光ディスク記録再生装置 3 0 0 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC の署名 TC Sig の検証を行う。当該検証において、光ディスク 1 2 が不正なものであると判定した場合は当該プロトコルを終了する。

【0 4 7 1】

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置 3 0 0 とセキュリティモジュール 5 3 の両方において正当であると判定した場合は、後段の手順 R 1 6 以降のデータ暗号化及び記録の処理に進むことになる。

【0 4 7 2】

次に、図 6 0 には、上記第 7 の実施の形態の光ディスク記録再生装置 3 0 0 が光ディスク 1 2 からデータを再生する手順を説明する。なお、図 6 0 の手順は、前記図 4 3 と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図 4 3 とは異なる部分のみ説明する。

【0 4 7 3】

この図 6 0 において、セキュリティモジュール 5 3 は、手順 P 1 2 の際に、乱数 R_A 、乱数 R_B 、値 V_A 、光ディスク 1 2 のデータ記録領域に記録されているリボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列に証明書 $Cert_A$ を付け、光ディスク記録再生装置 3 0 0 に送る。

【0 4 7 4】

これら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RevV_A$ 、 $RegV_A$ 、 Sig_A を受け取った光ディスク記録再生装置 3 0 0 は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 5 3 から返送されてきた乱数 R_B と先に生成したもののが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順 P 1 3 として、乱数 R_B 、乱数 R_A 、値 V_B 、自己がリストを持たないことを示す「0」のバージョンナンバーからなるビット列にデジタル署名を行い、これら R_B 、 R_A 、 V_B 、0、0、 Sig_B に証明書 $Cert_B$ を付け、セキ

リティモジュール 53 に送る。

【0475】

上記光ディスク記録再生装置 300 から $Cert_B$, R_B , R_A , V_B , 0, 0, Sig_B を受け取ると、セキュリティモジュール 53 は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

【0476】

ここで、セキュリティモジュール 53 にて当該検証をパスしたとき、すなわち、光ディスク記録再生装置 300 とセキュリティモジュール 53 の両方で検証をパスしたとき、セキュリティモジュール 53 と光ディスク記録再生装置 300 はセッション鍵 K_{se} を生成して共有する。

【0477】

次に、光ディスク記録再生装置 300 は、手順 P114 として、光ディスク 12 のデータ記録領域に格納されているリボケーションリスト／レジストレーションリストを読み取り、そのリストのバージョンナンバーが先の手順 P12 で取得したバージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いて光ディスク情報記録媒体 50 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC の署名 $TCSig$ の検証を行う。当該検証において、光ディスク情報記録媒体 50 が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、光ディスク記録再生装置 300 は、手順 P115 として、そのリストをセキュリティモジュール 53 に送る。なお、セキュリティモジュール 53 にリストを送るのは、検証の途中であっても良い。

【0478】

上記リストを受け取ったセキュリティモジュール 53 は、そのリストのバージョンナンバーが前記バージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いて光ディスク記録再生装置 300 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC の署名 $TCSig$ の検証を行う。当該検証において、光ディスク 12 が不正なものであると判定した場合は当該プロ

トコルを終了する。

【0 4 7 9】

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置 3 0 0 とセキュリティモジュール 5 3 の両方において正当であると判定した場合は、後段の手順 P 1 6 以降のデータ再生及び復号処理等に進むことになる。

【0 4 8 0】

次に、第 8 の実施の形態として、メディアタイプ IM 1 とデバイスタイプ Dev 2 の組み合わせ (IM 1, Dev 2) について説明する。

【0 4 8 1】

当該第 8 の実施の形態の組み合わせにおけるシステム構成は、図 6-1 に示すようになる。すなわち、デバイスタイプ Dev 2 の光ディスク記録再生装置 1 0 0 はリストを格納するための専用の前記不揮発性メモリ 1 1 0 を備えており、一方、メディアタイプ IM 1 の光ディスク情報記録媒体 5 0 のセキュリティモジュール 5 3 はリストを格納するための不揮発性メモリを備えていない。なお、当該図 6 1 における各部の構成は、前述の図 3 の例と同じであるため、それらの説明は省略する。

【0 4 8 2】

図 6 2 には、当該第 8 の実施の形態のメディアタイプ IM 1 とデバイスタイプ Dev 2 の組み合わせ (IM 1, Dev 2) の場合に、光ディスク記録再生装置 1 0 0 が光ディスク情報記録媒体 5 0 にデータを記録する手順を説明する。なお、図 6 2 において前述の各実施の形態の略々同じ手順についての説明は省略し、以下の説明では、それらと異なる部分のみ説明する。

【0 4 8 3】

図 6 2 は前記図 3 9 と略々同様な手順を表しており、手順 R 2 として、光ディスク記録再生装置 1 0 0 とセキュリティモジュール 5 3 との間でリボケーションリスト／レジストレーションリストのバージョンナンバーを交換する。当該第 8 の実施の形態の場合、光ディスク記録再生装置 1 0 0 は、不揮発性メモリ 1 1 0 にリボケーションリスト／レジストレーションリストを格納しているため、当該

リストのバージョンナンバーをセキュリティモジュール 53 に送り、また、光ディスク情報記録媒体 50 は、光ディスク 12 のコンテンツデータ記録用の領域に記録されているリボケーションリスト／レジストレーションリストのバージョンナンバーを光ディスク記録再生装置 100 に送ることになる。

【0484】

ここで、上記手順 R2 におけるリストのバージョンナンバーの交換により、光ディスク情報記録媒体 50 のリストのバージョンナンバーの方が、光ディスク記録再生装置 100 のリストのバージョンナンバーより新しい場合、光ディスク記録再生装置 100 は、手順 R123 として、光ディスク情報記録媒体 50 の光ディスク 12 のコンテンツデータ記録用の領域に記録されているリボケーションリスト／レジストレーションリストを読み出す。

【0485】

当該光ディスク記録再生装置 100 は、読み出したリストを用いて、当該光ディスク情報記録媒体 50 が正当なものであるか否か検証し、その検証の結果、当該光ディスク情報記録媒体 50 が不正なものであると判定した時は、当該プロトコルを終了する。一方、その光ディスク情報記録媒体 50 が正当であると判定した場合は、手順 R124 として、上記光ディスク 12 から読み出したリストをセキュリティモジュール 53 に送る。また、読み出したリストで自身のものを更新する。このときのセキュリティモジュール 53 は、当該リストを用いて、光ディスク記録再生装置 100 が正当であるか否かの検証を行い、不正である場合はプロトコルを終了する。

【0486】

上記セキュリティモジュール 53 が上記リストを用いた検証により正当であると判定した場合、すなわち、光ディスク記録再生装置 100 とセキュリティモジュール 53 の両者が共に正当であると判定した場合は、後段のデータ暗号化と記録の手順 R5 に進むことになる。

【0487】

また、上記手順 R2 におけるリストのバージョンナンバーの交換により、光ディスク記録再生装置 100 が保持するリストのバージョンナンバーが、光ディス

ク情報記録媒体 5 0 のリストのバージョンナンバーより新しいか又は同じである場合、光ディスク記録再生装置 1 0 0 は、手順 R 1 2 5 として、自己が不揮発性メモリ 1 1 0 に保持するリストをセキュリティモジュール 5 3 に送る。

【0 4 8 8】

このときのセキュリティモジュール 5 3 は、当該リストを用いて、上記光ディスク記録再生装置 1 0 0 が正当であるか否かの検証を行い、不正である場合はプロトコルを終了する。

【0 4 8 9】

上記セキュリティモジュール 5 3 が上記リストを用いた検証により正当であると判定した場合、すなわち、光ディスク記録再生装置 1 0 0 が正当であると判定した場合は、後段のデータ暗号化と記録の手順 R 5 に進むことになる。

【0 4 9 0】

また、上記手順 R 2 におけるリストのバージョンナンバーの交換により、光ディスク記録再生装置 1 0 0 が保持するリストのバージョンナンバーが、光ディスク情報記録媒体 5 0 のリストのバージョンナンバーより新しい場合、光ディスク記録再生装置 1 0 0 は、手順 R 1 2 6 として、自己が不揮発性メモリ 1 1 0 に保持するリストを、光ディスク 1 2 のデータ記録領域に記録する。この際、セキュリティモジュールは、そのバージョンナンバーを覚え、以後、使用する。

【0 4 9 1】

次に、図 6 3 には、上記図 6 2 に示した第 8 の実施の形態の光ディスク記録再生装置 1 0 0 が光ディスク情報記録媒体 5 0 にデータを記録するまでの手順の詳細を示している。なお、以下の説明では、前記図 4 1 の手順と異なる部分のみ説明する。

【0 4 9 2】

この図 6 3 において、セキュリティモジュール 5 3 は、手順 R 2 2 の際に、乱数 R_A 、乱数 R_B 、値 V_A 、光ディスク 1 2 のデータ記録領域に記録されているリボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列に証明書 $Cert_A$ を付け、光ディスク記録再生装置 1 0 0 に送る。

【0493】

これら $Cert_A$, R_A , R_B , V_A , $RevV_A$, $RegV_A$, Sig_A を受け取った光ディスク記録再生装置 100 は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 53 から返送されてきた乱数 R_B と先に生成したもののが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順 R 23 として、乱数 R_B 、乱数 R_A 、値 V_B 、自己の不揮発性メモリ 110 に格納しているリストのバージョンナンバー $RevV_B$, $RegV_B$ からなるビット列にデジタル署名を行い、これら R_B , R_A , V_B , $RevV_B$, $RegV_B$, Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール 53 に送る。

【0494】

上記光ディスク記録再生装置 100 から $Cert_B$, R_B , R_A , V_B , $RevV_B$, $RegV_B$, Sig_B を受け取ると、セキュリティモジュール 53 は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

【0495】

ここで、セキュリティモジュール 53 にて当該検証をパスしたとき、すなわち、光ディスク記録再生装置 100 とセキュリティモジュール 53 の両方で検証をパスしたとき、セキュリティモジュール 53 と光ディスク記録再生装置 100 はセッション鍵 K_{se} を生成して共有する。また、セキュリティモジュール 53 と光ディスク記録再生装置 100 は、それぞれリストのバージョンナンバーの新旧の検証を行う。

【0496】

上記リストのバージョンナンバーの新旧検証により、光ディスク情報記録媒体 50 のリストのバージョンナンバーの方が、光ディスク記録再生装置 100 のリストのバージョンナンバーより新しい場合、光ディスク記録再生装置 100 は、手順 R 134 として、光ディスク情報記録媒体 50 の光ディスク 12 のコンテンツデータ記録用の領域に記録されているリボケーションリスト／レジストレーションリストを読み出し、そのリストのバージョンナンバーが、先に取得したバージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いて

光ディスク情報記録媒体 50 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC の署名 TC Sig の検証を行う。当該検証において、光ディスク情報記録媒体 50 が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、光ディスク記録再生装置 300 は、手順 R 135 として、そのリストをセキュリティモジュール 53 に送ると共に、当該光ディスク 12 から読み取ったリストで自己の不揮発性メモリ 110 内のリストを更新する。なお、セキュリティモジュール 53 にリストを送るのは、検証の途中であっても良い。

【0497】

上記リストを受け取ったセキュリティモジュール 53 は、そのリストのバージョンナンバーが前記バージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いて光ディスク記録再生装置 100 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC の署名 TC Sig の検証を行う。当該検証において、光ディスク記録再生装置 100 が不正なものであると判定した場合は当該プロトコルを終了する。

【0498】

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置 100 とセキュリティモジュール 53 の両方において正当であると判定した場合は、後段の手順 R 26 以降のデータ暗号化及び記録の処理に進むことになる。

【0499】

また、上記リストのバージョンナンバーの新旧検証により、光ディスク記録再生装置 100 のリストのバージョンナンバーの方が、光ディスク情報記録媒体 50 のリストのバージョンナンバーより新しいか同一の場合、光ディスク記録再生装置 100 は、自己が保持するリストを用いて、光ディスク情報記録媒体 50 が正当か否か検証し、その検証でパスしたとき、手順 R 136 として、当該リストをセキュリティモジュール 53 に送る。なお、セキュリティモジュール 53 にリストを送るのは、検証の途中であっても良い。

【0500】

当該リストを受け取ったセキュリティモジュール53は、そのリストのバージョンナンバーが前記バージョンナンバー ($RevV_B$, $RegV_B$) と等しいこと、及び、当該リストを用いて光ディスク記録再生装置100が正当なものであるか否かの検証、当該リスト内に含まれるセンタTCの署名TCSigの検証を行う。当該検証において、光ディスク記録再生装置100が不正なものであると判定した場合は当該プロトコルを終了する。

【0501】

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置100とセキュリティモジュール53の両方において正当であると判定した場合は、後段の手順R26以降のデータ暗号化及び記録の処理に進むことになる。

【0502】

また、上記リストのバージョンナンバーの新旧検証により、光ディスク記録再生装置100が保持するリストのバージョンナンバーが、光ディスク情報記録媒体50のリストのバージョンナンバーより新しい場合、光ディスク記録再生装置100は、手順R137として、自己が不揮発性メモリ110に保持するリストを、光ディスク12のデータ記録領域に記録する。この際、セキュリティモジュールは、記憶しているバージョンナンバーを更新する。

【0503】

次に、図64には、上記第8の実施の形態の光ディスク記録再生装置100が光ディスク情報記録媒体50の光ディスク12からデータを再生する手順を説明する。なお、図64の手順は、前記図44と略々同様であり、以下の説明では、前記図44とは異なる部分のみ説明する。

【0504】

この図63において、セキュリティモジュール53は、手順P22の際に、乱数 R_A 、乱数 R_B 、値 V_A 、光ディスク12のデータ記録領域に記録されているリボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列に証明書 $Cert_A$ を付け、光ディ

スク記録再生装置 100 に送る。

【0505】

これら $Cert_A$, R_A , R_B , V_A , $RevV_A$, $RegV_A$, Sig_A を受け取った光ディスク記録再生装置 100 は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 53 から返送されてきた乱数 R_B と先に生成したもののが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順 P23 として、乱数 R_B 、乱数 R_A 、値 V_B 、自己の不揮発性メモリ 110 に格納しているリストのバージョンナンバー $RevV_B$, $RegV_B$ からなるビット列にデジタル署名を行い、これら R_B , R_A , V_B , $RevV_B$, $RegV_B$, Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール 53 に送る。

【0506】

上記光ディスク記録再生装置 100 から $Cert_B$, R_B , R_A , V_B , $RevV_B$, $RegV_B$, Sig_B を受け取ると、セキュリティモジュール 53 は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

【0507】

ここで、セキュリティモジュール 53 にて当該検証をパスしたとき、すなわち、光ディスク記録再生装置 100 とセキュリティモジュール 53 の両方で検証をパスしたとき、セキュリティモジュール 53 と光ディスク記録再生装置 100 はセッション鍵 K_{se} を生成して共有する。また、セキュリティモジュール 53 と光ディスク記録再生装置 100 は、それぞれリストのバージョンナンバーの新旧の検証を行う。

【0508】

上記リストのバージョンナンバーの新旧検証により、光ディスク情報記録媒体 50 のリストのバージョンナンバーの方が、光ディスク記録再生装置 100 のリストのバージョンナンバーより新しい場合、光ディスク記録再生装置 100 は、手順 P134 として、光ディスク情報記録媒体 50 の光ディスク 12 のコンテンツデータ記録用の領域に記録されているリボケーションリスト／レジストレーションリストを読み出し、そのリストのバージョンナンバーが、先に取得したバー

ジョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いて光ディスク情報記録媒体 50 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC の署名 TC Sig の検証を行う。当該検証において、光ディスク情報記録媒体 50 が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、光ディスク記録再生装置 300 は、手順 P 135 として、そのリストをセキュリティモジュール 53 に送ると共に、当該光ディスク 12 から読み取ったリストで自己の不揮発性メモリ 110 内のリストを更新する。なお、セキュリティモジュール 53 にリストを送るのは、検証の途中であっても良い。

【0509】

上記リストを受け取ったセキュリティモジュール 53 は、そのリストのバージョンナンバーが前記バージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いて光ディスク記録再生装置 100 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC の署名 TC Sig の検証を行う。当該検証において、光ディスク記録再生装置 100 が不正なものであると判定した場合は当該プロトコルを終了する。

【0510】

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置 100 とセキュリティモジュール 53 の両方において正当であると判定した場合は、後段の手順 P 26 以降のデータ再生及び復号の処理に進むことになる。

【0511】

また、上記リストのバージョンナンバーの新旧検証により、光ディスク記録再生装置 100 のリストのバージョンナンバーの方が、光ディスク情報記録媒体 50 のリストのバージョンナンバーより新しいか同一の場合、光ディスク記録再生装置 100 は、自己が保持するリストを用いて、光ディスク情報記録媒体 50 が正当か否か検証し、その検証でパスしたとき、手順 P 136 として、当該リストをセキュリティモジュール 53 に送る。なお、セキュリティモジュール 53 にリストを送るのは、検証の途中であっても良い。

【0512】

当該リストを受け取ったセキュリティモジュール53は、そのリストのバージョンナンバーが前記バージョンナンバー ($RevV_B$, $RegV_B$) と等しいこと、及び、当該リストを用いて光ディスク記録再生装置100が正当なものであるか否かの検証、当該リスト内に含まれるセンタTCの署名TCSigの検証を行う。当該検証において、光ディスク記録再生装置100が不正なものであると判定した場合は当該プロトコルを終了する。

【0513】

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置100とセキュリティモジュール53の両方において正当であると判定した場合は、後段の手順P26以降のデータ再生及び復号の処理に進むことになる。

【0514】

また、上記リストのバージョンナンバーの新旧検証により、光ディスク記録再生装置100が保持するリストのバージョンナンバーが、光ディスク情報記録媒体50のリストのバージョンナンバーより新しい場合、光ディスク記録再生装置100は、手順P137として、自己が不揮発性メモリ110に保持するリストを、光ディスク12のデータ記録領域に記録する。この際、セキュリティモジュールはバージョンナンバーを更新する。

【0515】

次に、第9の実施の形態として、メディアタイプIM2とデバイスタイプDev1の組み合わせ(IM2, Dev1)について説明する。

【0516】

当該第9の実施の形態の組み合わせにおけるシステム構成は、図65に示すようになる。すなわち、デバイスタイプDev1の光ディスク記録再生装置300はリストを格納するための専用の前記不揮発性メモリを備えておらず(但し、前述同様に鍵などのメモリは備えている)、メディアタイプIM2の光ディスク情報記録媒体10のセキュリティモジュール13はリストを格納するための不揮発性メモリ34を備えている。なお、当該図65における各部の構成は、前述の図

3の例と同じであるため、それらの説明は省略する。

【0517】

図66には、当該第9の実施の形態のメディアタイプIM2とデバイスタイプDev1の組み合わせ(IM2, Dev1)の場合に、光ディスク記録再生装置300が光ディスク情報記録媒体10にデータを記録する手順を説明する。なお、図66において前述の各実施の形態の略々同じ手順についての説明は省略し、以下の説明では、それらと異なる部分のみ説明する。

【0518】

図66は前記図39と略々同様な手順を表しており、手順R2として、光ディスク記録再生装置300とセキュリティモジュール13との間でリボケーションリスト/レジストレーションリストのバージョンナンバーを交換する。当該第9の実施の形態の場合、光ディスク記録再生装置300は、リボケーションリスト/レジストレーションリストを持たないため、当該リストのバージョンナンバーとして0をセキュリティモジュール13に送り、光ディスク情報記録媒体10は、セキュリティモジュール13内の不揮発性メモリ34に格納されているリストのバージョンナンバーを光ディスク記録再生装置300に送ることになる。

【0519】

ここで、上記手順R2におけるリストのバージョンナンバーの交換により、光ディスク記録再生装置300にはリストが存在しないため、セキュリティモジュール13は、不揮発性メモリ34に格納しているリストを用いて光ディスク記録再生装置300が正当なものであるか否か検証し、その検証の結果、当該光ディスク記録再生装置300が不正なものであると判定した時は、当該プロトコルを終了する。一方、その光ディスク記録再生装置300が正当であると判定した場合、セキュリティモジュール13は、手順R143として、上記不揮発性メモリ34に格納しているリボケーションリスト/レジストレーションリストを光ディスク記録再生装置300に送る。

【0520】

当該光ディスク記録再生装置300は、受け取ったリストを用いて、当該光ディスク情報記録媒体10が正当なものであるか否か検証し、その検証の結果、当

該光ディスク情報記録媒体 1 0 が不正なものであると判定した時は、当該プロトコルを終了する。一方、その光ディスク情報記録媒体 1 0 が正当であると判定した場合は、後段のデータ暗号化と記録の手順 R 5 に進むことになる。

【0 5 2 1】

次に、図 6 7 には、上記図 6 6 に示した第 9 の実施の形態の光ディスク記録再生装置 3 0 0 が光ディスク情報記録媒体 1 0 にデータを記録するまでの手順の詳細を示している。なお、以下の説明では、前記図 4 3 の手順と異なる部分のみ説明する。

【0 5 2 2】

この図 6 7 において、セキュリティモジュール 1 3 は、手順 R 1 2 の際に、乱数 R_A 、乱数 R_B 、値 V_A 、不揮発性メモリ 3 4 から読み出したリボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列に証明書 $Cert_A$ を付け、光ディスク記録再生装置 3 0 0 に送る。

【0 5 2 3】

これら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RevV_A$ 、 $RegV_A$ 、 Sig_A を受け取った光ディスク記録再生装置 3 0 0 は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 1 3 から返送されてきた乱数 R_B と先に生成したものとが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順 R 1 3 として、乱数 R_B 、乱数 R_A 、値 V_B 、リストを持たないことを示す「0」のバージョンナンバーからなるビット列にデジタル署名を行い、これら R_B 、 R_A 、 V_B 、0、0、 Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール 1 3 に送る。

【0 5 2 4】

上記光ディスク記録再生装置 3 0 0 から $Cert_B$ 、 R_B 、 R_A 、 V_B 、0、0、 Sig_B を受け取ると、セキュリティモジュール 1 3 は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行う。また、セキュリティモジュール 1 3 は、自己が保持するリストを用いて、光ディスク記録再生装置 3 0 0 が正当であるか否かの検証を行う。これら検証をパスしなかった場合は、当該プロトコルを終了する。

【0525】

ここで、セキュリティモジュール13にて上記検証をパスしたとき、すなわち、光ディスク記録再生装置300とセキュリティモジュール13の両方で上記検証をパスしたとき、セキュリティモジュール13と光ディスク記録再生装置300はセッション鍵 K_{se} を生成して共有する。

【0526】

次に、セキュリティモジュール13は、手順R154として、不揮発性メモリ34に格納しているリストを光ディスク記録再生装置300に送る。

【0527】

上記リストを受け取った光ディスク記録再生装置300は、そのリストのバージョンナンバーが前記バージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いて光ディスク情報記録媒体10が正当なものであるか否かの検証、当該リスト内に含まれるセンタTCの署名TCSigの検証を行う。当該検証において、光ディスク情報記録媒体10が不正なものであると判定した場合は当該プロトコルを終了する。

【0528】

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置300とセキュリティモジュール13の両方において正当であると判定した場合は、後段の手順R16以降のデータ暗号化及び記録の処理に進むことになる。

【0529】

次に、図68には、上記第9の実施の形態の光ディスク記録再生装置300が光ディスク情報記録媒体10の光ディスク12からデータを再生する手順を説明する。なお、図68の手順は、前記図60と略々同様であり、以下の説明では、前記図60とは異なる部分のみ説明する。

【0530】

この図68において、セキュリティモジュール13は、手順P12の際に、乱数 R_A 、乱数 R_B 、値 V_A 、不揮発性メモリ34から読み出したリボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナ

ンバー RegV_A からなるビット列に証明書 Cert_A を付け、光ディスク記録再生装置 3 0 0 に送る。

【0 5 3 1】

これら Cert_A , R_A , R_B , V_A , RevV_A , RegV_A , Sig_A を受け取った光ディスク記録再生装置 3 0 0 は、証明書 Cert_A 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 1 3 から返送されてきた乱数 R_B と先に生成したもののが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順 P 1 3 として、乱数 R_B 、乱数 R_A 、値 V_B 、リストを持たないことを示す「0」のバージョンナンバーからなるビット列にデジタル署名を行い、これら R_B , R_A , V_B , 0, 0, Sig_B に証明書 Cert_B を付け、セキュリティモジュール 1 3 に送る。

【0 5 3 2】

上記光ディスク記録再生装置 3 0 0 から Cert_B , R_B , R_A , V_B , 0, 0, Sig_B を受け取ると、セキュリティモジュール 1 3 は、証明書 Cert_B 、デジタル署名 Sig_B の検証を行う。また、セキュリティモジュール 1 3 は、自己が保持するリストを用いて、光ディスク記録再生装置 3 0 0 が正当であるか否かの検証を行う。これら検証をパスしなかった場合は、当該プロトコルを終了する。

【0 5 3 3】

ここで、セキュリティモジュール 1 3 にて上記検証をパスしたとき、すなわち、光ディスク記録再生装置 3 0 0 とセキュリティモジュール 1 3 の両方で上記検証をパスしたとき、セキュリティモジュール 1 3 と光ディスク記録再生装置 3 0 0 はセッション鍵 K_{se} を生成して共有する。

【0 5 3 4】

次に、セキュリティモジュール 1 3 は、手順 P 1 5 4 として、不揮発性メモリ 3 4 に格納しているリストを光ディスク記録再生装置 3 0 0 に送る。

【0 5 3 5】

上記リストを受け取った光ディスク記録再生装置 3 0 0 は、そのリストのバージョンナンバーが前記バージョンナンバー (RevV_A , RegV_A) と等しいこと、及び、当該リストを用いて光ディスク情報記録媒体 1 0 が正当なものであるか否

かの検証、当該リスト内に含まれるセンタTCの署名TCSigの検証を行う。当該検証において、光ディスク情報記録媒体10が不正なものであると判定した場合は当該プロトコルを終了する。

【0536】

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置300とセキュリティモジュール13の両方において正当であると判定した場合は、後段の手順P16以降のデータ再生及び復号の処理に進むことになる。

【0537】

次に、第10の実施の形態として、メディアタイプIM3とデバイスタイプDev3の組み合わせ(IM3, Dev3)から説明する。

【0538】

当該第10の実施の形態の組み合わせにおけるシステム構成は、図69に示ようになる。すなわち、デバイスタイプDev3のメモリ記録再生装置400はリストを格納するための専用の不揮発性メモリを備えておらず、また、メディアタイプIM3のメモリ情報記録媒体60のセキュリティモジュール63はリストを格納するための不揮発性メモリを備えていない。なお、当該図69における各部の構成は、前述の図14の例と同じであるため、それらの説明は省略する。

【0539】

図70には、当該第10の実施の形態のメディアタイプIM3とデバイスタイプDev3の組み合わせ(IM3, Dev3)の場合に、メモリ記録再生装置400がメモリ情報記録媒体60にデータを記録する手順を説明する。なお、図70において前述の各実施の形態の略々同じ手順についての説明は省略し、以下の説明では、それらと異なる部分のみ説明する。

【0540】

図70は前記図45と略々同様な手順を表しており、手順R32として、メモリ記録再生装置400とセキュリティモジュール63との間でリボケーションリスト/レジストレーションリストのバージョンナンバーを交換する。ここで、当該第10の実施の形態の場合は、メモリ記録再生装置400はリストを持たない

ため、バージョンナンバー 0 をセキュリティモジュール 6 3 に送り、また、メモリ情報記録媒体 6 0 はメモリ部 2 2 のコンテンツデータ記録用の領域に記録されているリボケーションリスト／レジストレーションリストのバージョンナンバーをメモリ記録再生装置 4 0 0 に送ることになる。

【0 5 4 1】

次に、セキュリティモジュール 6 0 は、手順 R 1 6 3 として、メモリ情報記録媒体 6 0 のメモリ部 2 2 のコンテンツデータ記録用の領域に記録されているリボケーションリスト／レジストレーションリストを読み出す。セキュリティモジュール 6 0 は、このリストを用いて、メモリ記録再生装置 4 0 0 が正当なものであるか否かの検証を行う。その検証の結果、当該メモリ記録再生装置 4 0 0 が不正なものであると判定した時は、当該プロトコルを終了する。一方、そのメモリ記録再生装置 4 0 0 が正当であると判定した場合は、手順 R 1 6 4 として、上記リストをメモリ記録再生装置 4 0 0 の送る。

【0 5 4 2】

当該メモリ記録再生装置 4 0 0 は、上記セキュリティモジュール 6 3 から送られたリストを用いて、当該メモリ情報記録媒体 6 0 が正当なものであるか否か検証し、その検証の結果、当該メモリ情報記録媒体 6 0 が不正なものであると判定した時は、当該プロトコルを終了する。

【0 5 4 3】

一方、上記検証において上記メモリ情報記録媒体 6 0 が正当であると判定した場合は、すなわち、メモリ記録再生装置 4 0 0 とメモリ情報記録媒体 6 0 の両者が共に正当であると判定された場合は、後段のデータ暗号化と記録の手順 R 3 5 に進むことになる。

【0 5 4 4】

次に、図 7 1 には、上記図 7 0 に示した第 1 0 の実施の形態のメモリ記録再生装置 4 0 0 がメモリ情報記録媒体 6 0 にデータを記録するまでの手順の詳細を示しており、前記図 4 6 と略々同様な手順となっている。

【0 5 4 5】

この図 7 1 において、セキュリティモジュール 6 3 は、手順 R 4 2 の際に、乱

数 R_A 、乱数 R_B 、値 V_A 、メモリ部のデータ記録領域から読み出したリボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列に証明書 $Cert_A$ を付け、メモリ記録再生装置 4 0 0 に送る。

【0 5 4 6】

これら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RevV_A$ 、 $RegV_A$ 、 Sig_A を受け取ったメモリ記録再生装置 4 0 0 は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 6 3 から返送されてきた乱数 R_B と先に生成したもののが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順 R 4 3 として、乱数 R_B 、乱数 R_A 、値 V_B 、自己がリストを持たないことを示す「0」のバージョンナンバーからなるビット列にデジタル署名を行い、これら R_B 、 R_A 、 V_B 、0、0、 Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール 6 3 に送る。

【0 5 4 7】

上記メモリ記録再生装置 4 0 0 から $Cert_B$ 、 R_B 、 R_A 、 V_B 、0、0、 Sig_B を受け取ると、セキュリティモジュール 6 3 は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

【0 5 4 8】

ここで、セキュリティモジュール 6 3 にて当該検証をパスしたとき、すなわち、メモリ記録再生装置 4 0 0 とセキュリティモジュール 6 3 の両方で検証をパスしたとき、セキュリティモジュール 6 3 とメモリ記録再生装置 4 0 0 はセッション鍵 K_{se} を生成して共有する。

【0 5 4 9】

次に、セキュリティモジュール 6 3 は、手順 R 1 6 4 として、メモリ部 2 2 のデータ記録領域に格納されているリボケーションリスト／レジストレーションリストを読み取り、そのリストのバージョンナンバーが先に取得したバージョンナンバー ($RevV_A$ 、 $RegV_A$) と等しいこと、及び、当該リストを用いてメモリ記録再生装置 4 0 0 が正当なものであるか否かの検証、当該リスト内に含まれるセ

ンタTCの署名TCSigの検証を行う。当該検証において、メモリ記録再生装置400が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、セキュリティモジュール63は、手順R165として、そのリストをメモリ記録再生装置400に送る。なお、メモリ記録再生装置400にリストを送るのは、検証の途中であっても良い。

【0550】

上記リストを受け取ったメモリ記録再生装置400は、そのリストのバージョンナンバーが先に取得したバージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いてメモリ情報記録媒体60が正当なものであるか否かの検証、当該リスト内に含まれるセンタTCの署名TCSigの検証を行う。当該検証において、メモリ情報記録媒体60が不正なものであると判定した場合は当該プロトコルを終了する。

【0551】

一方、この検証において正当なものであると判定した場合、すなわち、メモリ記録再生装置400とメモリ情報記録媒体60の両方において正当であると判定した場合は、後段の手順R46以降のデータ暗号化及び記録の処理に進むことになる。

【0552】

次に、図72には、上記第10の実施の形態のメモリ記録再生装置400がメモリ情報記録媒体60のメモリ部22からデータを再生する手順を説明する。なお、図72の手順は、前記図50と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図50とは異なる部分のみ説明する。

【0553】

この図72において、セキュリティモジュール63は、手順P42の際に、乱数 R_A 、乱数 R_B 、値 V_A 、メモリ部22のデータ記録領域から読み出したリボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列に証明書 $Cert_A$ を付け、メモリ記録再生装置400に送る。

【0554】

これら $Cert_A$, R_A , R_B , V_A , $RevV_A$, $RegV_A$, Sig_A を受け取ったメモリ記録再生装置400は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール63から返送されてきた乱数 R_B と先に生成したもののが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順P43として、乱数 R_B 、乱数 R_A 、値 V_B 、自己がリストを持たないことを示す「0」のバージョンナンバーからなるビット列にデジタル署名を行い、これら R_B , R_A , V_B , 0, 0, Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール63に送る。

【0555】

上記メモリ記録再生装置400から $Cert_B$, R_B , R_A , V_B , 0, 0, Sig_B を受け取ると、セキュリティモジュール63は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

【0556】

ここで、セキュリティモジュール63にて当該検証をパスしたとき、すなわち、メモリ記録再生装置400とセキュリティモジュール63の両方で検証をパスしたとき、セキュリティモジュール63とメモリ記録再生装置400はセッション鍵 K_{se} を生成して共有する。

【0557】

次に、セキュリティモジュール63は、手順P164として、メモリ部22のデータ記録領域に格納されているリボケーションリスト／レジストレーションリストを読み取り、そのリストのバージョンナンバーが先に取得したバージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いてメモリ記録再生装置400が正当なものであるか否かの検証、当該リスト内に含まれるセンタTCの署名 TC_{Sig} の検証を行う。当該検証において、メモリ記録再生装置400が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、セキュリティモジュール630は、手順P165として、そのリストをメモリ記録再生装置400に送る。

なお、メモリ記録再生装置 4 0 0 にリストを送るのは、検証の途中であっても良い。

【0 5 5 8】

上記リストを受け取ったメモリ記録再生装置 4 0 0 は、そのリストのバージョンナンバーが前記バージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いてメモリ情報記録媒体 6 0 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC の署名 TC Sig の検証を行う。当該検証において、メモリ情報記録媒体 6 0 が不正なものであると判定した場合は当該プロトコルを終了する。

【0 5 5 9】

一方、この検証において正当なものであると判定した場合、すなわち、メモリ記録再生装置 4 0 0 とセキュリティモジュール 6 3 の両方において正当であると判定した場合は、後段の手順 P 4 6 以降のデータ再生及び復号処理等に進むことになる。

【0 5 6 0】

次に、第 1 1 の実施の形態として、メディアタイプ IM 3 とデバイスタイプ Dev 4 の組み合わせ (IM 3, Dev 4) について説明する。

【0 5 6 1】

当該第 1 1 の実施の形態の組み合わせにおけるシステム構成は、図 7 3 に示ようになる。すなわち、デバイスタイプ Dev 4 のメモリ記録再生装置 2 0 0 はリストを格納するための専用の前記不揮発性メモリ 2 1 0 を備えており、一方、メディアタイプ IM 3 のメモリ情報記録媒体 6 0 のセキュリティモジュール 6 3 はリストを格納するための不揮発性メモリを備えていない。なお、当該図 7 3 における各部の構成は、前述の図 1 4 の例と同じであるため、それらの説明は省略する。

【0 5 6 2】

図 7 4 には、当該第 1 1 の実施の形態のメディアタイプ IM 3 とデバイスタイプ Dev 4 の組み合わせ (IM 3, Dev 4) の場合に、メモリ記録再生装置 2 0 0 がメモリ情報記録媒体 6 0 にデータを記録する手順を説明する。なお、図 7

4において前述の各実施の形態の略々同じ手順についての説明は省略し、以下の説明では、それらと異なる部分のみ説明する。

【0563】

図74は前記図45と略々同様な手順を表しており、手順R32として、メモリ記録再生装置200とセキュリティモジュール63との間でリボケーションリスト／レジストレーションリストのバージョンナンバーを交換する。当該第11の実施の形態の場合、メモリ記録再生装置200は、不揮発性メモリ210にリボケーションリスト／レジストレーションリストを格納しているため、当該リストのバージョンナンバーをセキュリティモジュール63に送り、また、メモリ情報記録媒体60は、メモリ部22のコンテンツデータ記録用の領域に記録されているリボケーションリスト／レジストレーションリストのバージョンナンバーをメモリ記録再生装置200に送ることになる。

【0564】

ここで、上記手順R32におけるリストのバージョンナンバーの交換により、メモリ情報記録媒体60のメモリ部22に記録されているリストのバージョンナンバーが、メモリ記録再生装置200が保持するリストのバージョンナンバーより新しいか又は同じである場合、セキュリティモジュール63は、手順R173として、メモリ部22に記録されているリストを読み出す。当該セキュリティモジュール63は、当該リストを用いて、上記メモリ記録再生装置200が正当なものであるか否か検証し、その検証の結果、当該メモリ記録再生装置200が不正なものであると判定した時は、当該プロトコルを終了する。

【0565】

一方、そのメモリ記録再生装置200が正当であると判定した場合は、すなわち、メモリ記録再生装置200とセキュリティモジュール63の両者が共に正当であると判定した場合は、後段のデータ暗号化と記録の手順R35に進むことになる。また、セキュリティモジュール63は、手順R174として、上記リストをメモリ記録再生装置200に送る。

【0566】

当該メモリ記録再生装置200は、上記供給されたリストを用いて、当該メモ

リ情報記録媒体 60 が正当なものであるか否か検証し、その検証の結果、当該メモリ情報記録媒体 60 が不正なものであると判定した時は、当該プロトコルを終了する。一方、そのメモリ情報記録媒体 60 が正当であると判定した場合は、後段のデータ暗号化と記録の手順 R 35 に進むことになる。

【0567】

また、上記手順 R 32 におけるリストのバージョンナンバーの交換により、メモリ記録再生装置 200 が保持するリストのバージョンナンバーが、メモリ情報記録媒体 60 のメモリ部 22 に記録されているリストのバージョンナンバーより新しい場合、メモリ記録再生装置 200 は、手順 R 175 として、自己が保持するリストをセキュリティモジュール 63 に送る。セキュリティモジュール 63 は、当該リストを用いて、上記メモリ記録再生装置 200 が正当なものであるか否か検証し、その検証の結果、当該メモリ記録再生装置 200 が不正なものであると判定した時は、当該プロトコルを終了する。

【0568】

一方、そのメモリ記録再生装置 200 が正当であると判定した場合は、セキュリティモジュール 63 は、手順 R 176 として、上記メモリ記録再生装置 200 から供給されたリストをメモリ部 22 のデータ記録領域に記録させると共に、手順 R 35 に進む。

【0569】

次に、図 75 には、上記図 74 に示した第 11 の実施の形態のメモリ記録再生装置 200 がメモリ情報記録媒体 60 にデータを記録するまでの手順の詳細を示している。なお、以下の説明では、前記図 47 の手順と異なる部分のみ説明する。

【0570】

この図 75 において、セキュリティモジュール 63 は、手順 R 52 の際に、乱数 R_A 、乱数 R_B 、値 V_A 、メモリ部 22 のデータ記録領域から読み出したリボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列に証明書 $Cert_A$ を付け、メモリ記録再生装置 200 に送る。

【0571】

これら $Cert_A$, R_A , R_B , V_A , $RevV_A$, $RegV_A$, Sig_A を受け取ったメモリ記録再生装置 200 は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 63 から返送されてきた乱数 R_B と先に生成したもののが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順 R53 として、乱数 R_B 、乱数 R_A 、値 V_B 、自己の不揮発性メモリ 210 に格納しているリストのバージョンナンバー $RevV_B$, $RegV_B$ からなるビット列にデジタル署名を行い、これら R_B , R_A , V_B , $RevV_B$, $RegV_B$, Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール 63 に送る。

【0572】

上記メモリ記録再生装置 200 から $Cert_B$, R_B , R_A , V_B , $RevV_B$, $RegV_B$, Sig_B を受け取ると、セキュリティモジュール 63 は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

【0573】

ここで、セキュリティモジュール 63 にて当該検証をパスしたとき、すなわち、メモリ記録再生装置 200 とセキュリティモジュール 63 の両方で検証をパスしたとき、セキュリティモジュール 63 とメモリ記録再生装置 200 はセッション鍵 K_{se} を生成して共有する。

【0574】

また、セキュリティモジュール 63 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 63 とメモリ記録再生装置 200 は、それぞれリストのバージョンナンバーのチェックを行う。

【0575】

ここで、両者のバージョンナンバーが同じである場合、セキュリティモジュール 63 は、手順 R184 として、メモリ部 22 からリストを読み出し、そのリストのバージョンナンバーが先に取得したバージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いてメモリ記録再生装置 200 が正当な

ものであるか否かの検証、当該リスト内に含まれるセンタTCの署名TCSigの検証を行う。当該検証において、メモリ記録再生装置200が不正なものであると判定した場合は当該プロトコルを終了する。また、この時のメモリ記録再生装置200は、自己が保持するリストを用いて、メモリ情報記録媒体60が正当であるか否かの検証を行い、不正なものであると判定したときは当該プロトコルを終了し、これらセキュリティモジュール63及びメモリ記録再生装置200において、共に正当であると判定した時は、その後の手順R56以降に進むことになる。

【0576】

また、両者のバージョンナンバーの検証を行った結果、メモリ情報記録媒体60のメモリ部22が保持するリストのバージョンナンバーが、メモリ記録再生装置200が保持するリストのバージョンナンバーより新しい場合、セキュリティモジュール63は、手順R185として、メモリ部22からリストを読み出し、そのリストのバージョンナンバーが先に取得したバージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いてメモリ記録再生装置200が正当なものであるか否かの検証、当該リスト内に含まれるセンタTCの署名TCSigの検証を行う。当該検証において、メモリ記録再生装置200が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ記録再生装置200が正当であると判定した場合は、手順R186として、上記リストをメモリ記録再生装置200の送る。

【0577】

メモリ記録再生装置200は、当該リストを受け取ると、そのリストのバージョンナンバーが先に取得したバージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いてメモリ情報記録媒体60が正当なものであるか否かの検証、当該リスト内に含まれるセンタTCの署名TCSigの検証を行う。当該検証において、メモリ情報記録媒体60が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ情報記録媒体60が正当であると判定した場合は、その後の手順R56以降に進むことになる。

【0578】

また、両者のバージョンナンバーの検証を行った結果、メモリ記録再生装置 200 が保持するリストのバージョンナンバーが、メモリ情報記録媒体 60 のメモリ部 22 が保持するリストのバージョンナンバーより新しい場合、メモリ記録再生装置 200 は、当該リストを用いてメモリ情報記録媒体 60 が正当なものであるか否かを検証し、当該検証において、メモリ情報記録媒体 60 が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ情報記録媒体 60 が正当であると判定した場合は、手順 R187 として、上記リストをセキュリティモジュール 63 に送る。

【0579】

~~セキュリティモジュール 63 は、当該リストを受け取ると、そのリストのバージョンナンバーが先に取得したバージョンナンバー ($RevV_B$, $RegV_B$) と等しいこと、及び、当該リストを用いてメモリ記録再生装置 200 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC の署名 TC Sig の検証を行う。~~当該検証において、メモリ記録再生装置 200 が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ記録再生装置 200 が正当であると判定した場合は、手順 R188 として、上記リストをメモリ部 22 に書き込んで更新し、その後の手順 R56 以降に進むことになる。なお、リストの更新と手順 R56 以降の処理は前後してもかまわない。これらのメディアタイプ IM3 では、メモリに格納されているリストのバージョンをプロトコル中で読み出すようにしているが、メモリ上でのリストの改ざんを防止するために、バージョンナンバーをセキュリティモジュールが記憶しておくことが望ましい。

【0580】

次に、図 76 には、上記第 11 の実施の形態のメモリ記録再生装置 200 がメモリ情報記録媒体 60 のメモリ部 22 からデータを再生する手順を説明する。なお、図 76 の手順は、前記図 51 と略々同様であり、以下の説明では、前記図 51 とは異なる部分のみ説明する。

【0581】

この図 76 において、セキュリティモジュール 63 は、手順 P52 の際に、乱

数 R_A 、乱数 R_B 、値 V_A 、メモリ部 2 2 のデータ記録領域から読み出したリボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列に証明書 $Cert_A$ を付け、メモリ記録再生装置 2 0 0 に送る。

【0 5 8 2】

これら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RevV_A$ 、 $RegV_A$ 、 Sig_A を受け取ったメモリ記録再生装置 2 0 0 は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 6 3 から返送されてきた乱数 R_B と先に生成したもののが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順 P 5 3 として、乱数 R_B 、乱数 R_A 、値 V_B 、自己の不揮発性メモリ 2 1 0 に格納しているリストのバージョンナンバー $RevV_B$ 、 $RegV_B$ からなるビット列にデジタル署名を行い、これら R_B 、 R_A 、 V_B 、 $RevV_B$ 、 $RegV_B$ 、 Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール 6 3 に送る。

【0 5 8 3】

上記メモリ記録再生装置 2 0 0 から $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RevV_B$ 、 $RegV_B$ 、 Sig_B を受け取ると、セキュリティモジュール 6 3 は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

【0 5 8 4】

ここで、セキュリティモジュール 6 3 にて当該検証をパスしたとき、すなわち、メモリ記録再生装置 2 0 0 とセキュリティモジュール 6 3 の両方で検証をパスしたとき、セキュリティモジュール 6 3 とメモリ記録再生装置 2 0 0 はセッション鍵 K_{se} を生成して共有する。

【0 5 8 5】

また、セキュリティモジュール 6 3 とメモリ記録再生装置 2 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 6 3 とメモリ記録再生装置 2 0 0 は、それぞれリストのバージョンナンバーのチェックを行う。

【0 5 8 6】

ここで、両者のバージョンナンバーが同じである場合、セキュリティモジュール 6 3 は、手順 P 1 8 4 として、メモリ部 2 2 からリストを読み出し、そのリストのバージョンナンバーが先に取得したバージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いてメモリ記録再生装置 2 0 0 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC の署名 TC Sig の検証を行う。当該検証において、メモリ記録再生装置 2 0 0 が不正なものであると判定した場合は当該プロトコルを終了する。また、この時のメモリ記録再生装置 2 0 0 は、自己が保持するリストを用いて、メモリ情報記録媒体 6 0 が正当であるか否かの検証を行い、不正なものであると判定したときは当該プロトコルを終了し、これらセキュリティモジュール 6 3 及びメモリ記録再生装置 2 0 0 において、共に正当であると判定した時は、その後の手順 R 5 6 以降に進むことになる。

【0 5 8 7】

また、両者のバージョンナンバーの検証を行った結果、メモリ情報記録媒体 6 0 のメモリ部 2 2 が保持するリストのバージョンナンバーが、メモリ記録再生装置 2 0 0 が保持するリストのバージョンナンバーより新しい場合、セキュリティモジュール 6 3 は、手順 P 1 8 5 として、メモリ部 2 2 からリストを読み出し、そのリストのバージョンナンバーが先に取得したバージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いてメモリ記録再生装置 2 0 0 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC の署名 TC Sig の検証を行う。当該検証において、メモリ記録再生装置 2 0 0 が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ記録再生装置 2 0 0 が正当であると判定した場合は、手順 P 1 8 6 として、上記リストをメモリ記録再生装置 2 0 0 の送る。

【0 5 8 8】

メモリ記録再生装置 2 0 0 は、当該リストを受け取ると、そのリストのバージョンナンバーが先に取得したバージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いてメモリ情報記録媒体 6 0 が正当なものであるか

否かの検証、当該リスト内に含まれるセンタTCの署名TCSigの検証を行う。
当該検証において、メモリ情報記録媒体60が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ情報記録媒体60が正当であると判定した場合は、その後の手順P56以降に進むことになる。

【0589】

また、両者のバージョンナンバーの検証を行った結果、メモリ記録再生装置200が保持するリストのバージョンナンバーが、メモリ情報記録媒体60のメモリ部22が保持するリストのバージョンナンバーより新しい場合、メモリ記録再生装置200は、当該リストを用いてメモリ情報記録媒体60が正当なものであるか否かを検証し、当該検証において、メモリ情報記録媒体60が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ情報記録媒体60が正当であると判定した場合は、手順P187として、上記リストをセキュリティモジュール63に送る。

【0590】

セキュリティモジュール63は、当該リストを受け取ると、そのリストのバージョンナンバーが先に取得したバージョンナンバー ($RevV_B$, $RegV_B$) と等しいこと、及び、当該リストを用いてメモリ記録再生装置200が正当なものであるか否かの検証、当該リスト内に含まれるセンタTCの署名TCSigの検証を行う。当該検証において、メモリ記録再生装置200が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ記録再生装置200が正当であると判定した場合は、手順P188として、上記リストをメモリ部22に書き込んで更新し、その後の手順P56以降に進むことになる。なお、リストの更新と手順P56以降の処理は前後してもかまわない。

【0591】

次に、第12の実施の形態として、メディアタイプIM4とデバイスタイプDev3の組み合わせ(IM4, Dev3)について説明する。

【0592】

当該第12の実施の形態の組み合わせにおけるシステム構成は、図77に示ようになる。すなわち、デバイスタイプDev3のメモリ記録再生装置400は

リストを格納するための専用の前記不揮発性メモリを備えておらず、一方、メディアタイプIM4のメモリ情報記録媒体20のセキュリティモジュール23はリストを格納するための不揮発性メモリ43を備えている。なお、当該図77における各部の構成は、前述の図14の例と同じであるため、それらの説明は省略する。

【0593】

図78には、当該第12の実施の形態のメディアタイプIM4とデバイスタイプDev3の組み合わせ(IM4, Dev3)の場合に、メモリ記録再生装置400がメモリ情報記録媒体10にデータを記録する手順を説明する。なお、図78において前述の各実施の形態の略々同じ手順についての説明は省略し、以下の説明では、それらと異なる部分のみ説明する。

【0594】

図78は前記図45と略々同様な手順を表しており、手順R32として、メモリ記録再生装置400とセキュリティモジュール23との間でリボケーションリスト/レジストレーションリストのバージョンナンバーを交換する。当該第12の実施の形態の場合、メモリ記録再生装置200は、リボケーションリスト/レジストレーションリストを持たないため、当該リストのバージョンナンバーとして「0」をセキュリティモジュール23に送り、メモリ情報記録媒体20は、セキュリティモジュール23内の不揮発性メモリ44に格納されているリストのバージョンナンバーをメモリ記録再生装置400に送ることになる。

【0595】

ここで、上記手順R32におけるリストのバージョンナンバーの交換により、メモリ記録再生装置400にはリストが存在しないため、セキュリティモジュール23は、不揮発性メモリ44に格納しているリストを用いてメモリ記録再生装置400が正当なものであるか否か検証し、その検証の結果、当該メモリ記録再生装置400が不正なものであると判定した時は、当該プロトコルを終了する。一方、そのメモリ記録再生装置400が正当であると判定した場合、セキュリティモジュール23は、手順R193として、上記不揮発性メモリ44に格納しているリボケーションリスト/レジストレーションリストをメモリ記録再生装置4

0 0 に送る。

【0 5 9 6】

当該メモリ記録再生装置 4 0 0 は、受け取ったリストを用いて、当該メモリ情報記録媒体 2 0 が正当なものであるか否か検証し、その検証の結果、当該メモリ情報記録媒体 2 0 が不正なものであると判定した時は、当該プロトコルを終了する。一方、そのメモリ情報記録媒体 2 0 が正当であると判定した場合は、後段のデータ暗号化と記録の手順 R 3 5 に進むことになる。

【0 5 9 7】

次に、図 7 9 には、上記図 7 8 に示した第 1 2 の実施の形態のメモリ記録再生装置 4 0 0 がメモリ情報記録媒体 2 0 にデータを記録するまでの手順の詳細を示している。~~なお、以下の説明では、前記図 4 6 の手順と異なる部分のみ説明する。~~

【0 5 9 8】

この図 7 9 において、セキュリティモジュール 2 3 は、手順 R 4 2 の際に、乱数 R_A 、乱数 R_B 、値 V_A 、不揮発性メモリ 4 4 から読み出したリボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列に証明書 $Cert_A$ を付け、メモリ記録再生装置 4 0 0 に送る。

【0 5 9 9】

これら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RevV_A$ 、 $RegV_A$ 、 Sig_A を受け取ったメモリ記録再生装置 4 0 0 は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール 2 3 から返送されてきた乱数 R_B と先に生成したもののが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順 R 4 3 として、乱数 R_B 、乱数 R_A 、値 V_B 、リストを持たないことを示す「0」のバージョンナンバーからなるビット列にデジタル署名を行い、これら R_B 、 R_A 、 V_B 、0、0、 Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール 2 3 に送る。

【0 6 0 0】

上記メモリ記録再生装置 4 0 0 から $Cert_B$ 、 R_B 、 R_A 、 V_B 、0、0、 Sig_B を

受け取ると、セキュリティモジュール 23 は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行う。また、セキュリティモジュール 23 は、自己が保持するリストを用いて、メモリ記録再生装置 400 が正当であるか否かの検証を行う。これら検証をパスしなかった場合は、当該プロトコルを終了する。

【0601】

ここで、セキュリティモジュール 23 にて上記検証をパスしたとき、すなわち、メモリ記録再生装置 400 とセキュリティモジュール 23 の両方で上記検証をパスしたとき、セキュリティモジュール 23 とメモリ記録再生装置 400 はセッション鍵 K_{se} を生成して共有する。

【0602】

~~次に、セキュリティモジュール 23 は、手順 R204 として、不揮発性メモリ 44 に格納しているリストをメモリ記録再生装置 400 に送る。~~

【0603】

上記リストを受け取ったメモリ記録再生装置 400 は、そのリストのバージョンナンバーが前記バージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いてメモリ情報記録媒体 20 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC の署名 TC_{Sig} の検証を行う。当該検証において、メモリ情報記録媒体 20 が不正なものであると判定した場合は当該プロトコルを終了する。

【0604】

一方、この検証において正当なものであると判定した場合、すなわち、メモリ記録再生装置 400 とセキュリティモジュール 23 の両方において正当であると判定した場合は、後段の手順 R46 以降のデータ暗号化及び記録の処理に進むことになる。

【0605】

次に、図 80 には、上記第 12 の実施の形態のメモリ記録再生装置 400 がメモリ情報記録媒体 20 のメモリ部 22 からデータを再生する手順を説明する。なお、図 80 の手順は、前記図 50 と略々同様であり、以下の説明では、前記図 50 とは異なる部分のみ説明する。

【0606】

この図80において、セキュリティモジュール23は、手順P42の際に、乱数 R_A 、乱数 R_B 、値 V_A 、不揮発性メモリ44から読み出したリボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列に証明書 $Cert_A$ を付け、メモリ記録再生装置400に送る。

【0607】

これら $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RevV_A$ 、 $RegV_A$ 、 Sig_A を受け取ったメモリ記録再生装置400は、証明書 $Cert_A$ 、デジタル署名 Sig_A の検証を行い、その検証をパスし、さらに、セキュリティモジュール23から返送されてきた乱数 R_B と先に生成したものが等しく、且つデジタル署名 Sig_A が正当であると判定されたとき、手順P43として、乱数 R_B 、乱数 R_A 、値 V_B 、リストを持たないことを示す「0」のバージョンナンバーからなるビット列にデジタル署名を行い、これら R_B 、 R_A 、 V_B 、0、0、 Sig_B に証明書 $Cert_B$ を付け、セキュリティモジュール23に送る。

【0608】

上記メモリ記録再生装置400から $Cert_B$ 、 R_B 、 R_A 、 V_B 、0、0、 Sig_B を受け取ると、セキュリティモジュール23は、証明書 $Cert_B$ 、デジタル署名 Sig_B の検証を行う。また、セキュリティモジュール23は、自己が保持するリストを用いて、メモリ記録再生装置400が正当であるか否かの検証を行う。これら検証をパスしなかった場合は、当該プロトコルを終了する。

【0609】

ここで、セキュリティモジュール23にて上記検証をパスしたとき、すなわち、メモリ記録再生装置400とセキュリティモジュール23の両方で上記検証をパスしたとき、セキュリティモジュール23とメモリ記録再生装置400はセッション鍵 K_{se} を生成して共有する。

【0610】

次に、セキュリティモジュール23は、手順P204として、不揮発性メモリ44に格納しているリストをメモリ記録再生装置400に送る。

【0611】

上記リストを受け取ったメモリ記録再生装置400は、そのリストのバージョンナンバーが前記バージョンナンバー ($RevV_A$, $RegV_A$) と等しいこと、及び、当該リストを用いてメモリ情報記録媒体20が正当なものであるか否かの検証、当該リスト内に含まれるセンタTCの署名TCSigの検証を行う。当該検証において、メモリ情報記録媒体20が不正なものであると判定した場合は当該プロトコルを終了する。

【0612】

一方、この検証において正当なものであると判定した場合、すなわち、メモリ記録再生装置400とセキュリティモジュール23の両方において正当であると判定した場合は、後段の手順P16以降のデータ再生及び復号の処理に進むことになる。

【0613】

次に、図81～図87のフローチャートを用いて、本発明の各実施の形態のセキュリティモジュールと記録再生装置が、それぞれタイプ別に行う処理の流れを説明する。なお、以下の説明では、リボケーションリスト/レジストレーションリストの両方を用いた場合を例に挙げている。

【0614】

図81には、前記メディアタイプIM1に相当する光ディスク情報記録媒体50のセキュリティモジュール53における処理の流れを示す。

【0615】

この図81において、セキュリティモジュール53は、ステップS1として、前述したように、光ディスク記録再生装置が発生した乱数 R_B の受信と、前記 $V_A = K_A \cdot G$ の計算、乱数 R_A の発生、デジタル署名を行い Sig_A 計算、 $Cert_A$, R_A , R_B , V_A , $RevV_A$, $RegV_A$, Sig_A を光ディスク記録再生装置に送信する。

【0616】

次に、セキュリティモジュール53は、ステップS2として、光ディスク記録再生装置から送信されてきた $Cert_B$, R_B , R_A , V_B , $RevV_B$, $RegV_B$, Sig_B 受信、 $Cert_B$ の検証、 Sig_B の検証、セッション鍵 K_{se} の計算を行う。

【0 6 1 7】

次に、セキュリティモジュール 5 3 は、ステップ S 3 として、例えばリストのバージョンナンバーが「0」か否かにより、相手方の光ディスク記録再生装置のデバイスタイプを判定する。このステップ S 3 の判定において、例えばリストのバージョンナンバーが「0」となっており、前記デバイスタイプ Dev 1（すなわち前記光ディスク記録再生装置 3 0 0）であると判定した場合、セキュリティモジュール 5 3 の処理は、ステップ S 4 に進む。一方、ステップ S 3 の判定において、リストのバージョンナンバーが「0」でなく、前記デバイスタイプ Dev 2（すなわち前記光ディスク記録再生装置 1 0 0）であると判定した場合、セキュリティモジュール 5 3 の処理は、ステップ S 5 に進む。

【0 6 1 8】

ステップ S 4 の処理に進むと、セキュリティモジュール 5 3 は、光ディスク 1 2 のデータ記録領域からリボケーションリスト／レジストレーションリストを読み取り、そのバージョンナンバー（RevV_A, RegV_A）の検証と、そのリストを用いた光ディスク記録再生装置（デバイスタイプ Dev 1 の装置 3 0 0）の ID_B の検証と、センタ TC の署名 TCSig の検証を行った後、ステップ S 8 に進む。

【0 6 1 9】

また、ステップ S 5 の処理に進むと、セキュリティモジュール 5 3 は、光ディスク 1 2 のデータ記録領域に記録されているリボケーションリスト／レジストレーションリストのバージョンが、デバイスタイプ Dev 2 の光ディスク記録再生装置 1 0 0 の保持するリストのバージョンナンバーよりも大きい（ $A > B$ ）か、或いはそれ以下（ $A \leq B$ ）であるのかの判定を行う。このステップ S 5 の判定において、 $A > B$ であると判定した場合、セキュリティモジュール 5 3 の処理はステップ S 6 に進み、一方、 $A \leq B$ であると判定した場合、セキュリティモジュール 5 3 の処理はステップ S 7 に進む。

【0 6 2 0】

ステップ S 6 の処理に進むと、セキュリティモジュール 5 3 は、光ディスク 1 2 のデータ記録領域からリボケーションリスト／レジストレーションリストを読み取り、そのバージョンナンバー（RevV_A, RegV_A）の検証と、そのリストを

用いた光ディスク記録再生装置 100 の ID_B の検証と、センタ TC の署名 $TCSig$ の検証を行った後、ステップ S8 に進む。

【0621】

また、ステップ S7 の処理に進むと、セキュリティモジュール 53 は、光ディスク記録再生装置 100 が保持するリボケーションリスト／レジストレーションリストを受け取り、そのバージョンナンバー ($RevV_B$, $RegV_B$) の検証と、そのリストを用いた光ディスク記録再生装置 100 の ID_B の検証と、センタ TC の署名 $TCSig$ の検証を行った後、ステップ S8 に進む。

【0622】

ステップ S8 の処理に進むと、セキュリティモジュール 53 は、光ディスク記録再生装置から記録又は再生の何れの処理が要求されているのか判定する。

【0623】

当該ステップ S8 にて記録の処理が要求されていると判定した場合、セキュリティモジュール 53 は、ステップ S9 の処理として、光ディスク記録再生装置がセッション鍵 K_{se} にて暗号鍵 K_{co} を暗号化した値 $Enc(K_{se}, K_{co})$ を受信して復号し、次に、その復号により得られた暗号鍵 K_{co} を自己が保持するストレージ鍵 K_{st} で暗号化した値 $Enc(K_{st}, K_{co})$ を生成して光ディスク記録再生装置に送信する。その後、光ディスク記録再生装置において上記暗号鍵 K_{co} にて暗号化されたコンテンツデータ $Enc(K_{se}, K_{co})$ が、光ディスク 12 に記録されることになる。

【0624】

一方、ステップ S8 にて再生の処理が要求されていると判定した場合、セキュリティモジュール 53 は、ステップ S10 の処理として、ストレージ鍵 K_{st} にて暗号鍵 K_{co} が暗号化され例えば光ディスク 12 のデータ記録領域等に記録されている値 $Enc(K_{st}, K_{co})$ を読み出して復号し、その復号により得られた暗号鍵 K_{co} をセッション鍵 K_{se} にて暗号化した値 $Enc(K_{se}, K_{co})$ を生成して光ディスク記録再生装置に送信する。その後、上記暗号鍵 K_{co} にて暗号化されているコンテンツデータ $Enc(K_{se}, K_{co})$ は、光ディスク 12 から再生されて光ディスク記録再生装置に送られることになる。

【0625】

図82には、前記メディアタイプIM2に相当する光ディスク情報記録媒体10のセキュリティモジュール13における処理の流れを示す。

【0626】

この図82において、セキュリティモジュール13は、ステップS11として、前述したように、光ディスク記録再生装置が発生した乱数 R_B の受信と、前記 $V_A = K_A \cdot G$ の計算、乱数 R_A の発生、デジタル署名を行い Sig_A 計算、 $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RevV_A$ 、 $RegV_A$ 、 Sig_A を光ディスク記録再生装置に送信する。

【0627】

次に、セキュリティモジュール13は、ステップS12として、光ディスク記録再生装置から送信されてきた $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RevV_B$ 、 $RegV_B$ 、 Sig_B 受信、 $Cert_B$ の検証、 Sig_B の検証、セッション鍵 K_{se} の計算を行う。

【0628】

次に、セキュリティモジュール13は、ステップS13として、例えばリストのバージョンナンバーが「0」か否かにより、相手方の光ディスク記録再生装置のデバイスタイプを判定する。このステップS13の判定において、例えばリストのバージョンナンバーが「0」となっており、前記デバイスタイプDev1（光ディスク記録再生装置300）であると判定した場合、セキュリティモジュール13の処理は、ステップS14に進む。一方、ステップS13の判定において、リストのバージョンナンバーが「0」でなく、前記デバイスタイプDev2（光ディスク記録再生装置100）であると判定した場合、セキュリティモジュール13の処理は、ステップS15に進む。

【0629】

ステップS14の処理に進むと、セキュリティモジュール13は、不揮発性メモリ34に格納しているリストを用いて光ディスク記録再生装置300の ID_B を検証し、その検証をパスしたとき、上記リストを光ディスク記録再生装置300に送信した後、ステップS19の処理に進む。

【0630】

また、ステップS15の処理に進むと、セキュリティモジュール13は、不揮発性メモリ34に格納しているリストのバージョンが、光ディスク記録再生装置100が保持するリストのバージョンナンバーよりも大きい($A > B$)か、或いは等しいか($A = B$)、或いは小さいか($A < B$)の判定を行う。このステップS15の判定において、 $A > B$ であると判定した場合、セキュリティモジュール13の処理はステップS16に進み、 $A = B$ であると判定した場合、セキュリティモジュール13の処理はステップS17に進み、 $A < B$ であると判定した場合、セキュリティモジュール13の処理はステップS18に進む。

【0631】

~~ステップS16の処理に進むと、セキュリティモジュール13は、自己が保持するリストを用いて光ディスク記録再生装置100のID_Bの検証を行い、そのリストを光ディスク記録再生装置100に送信した後、ステップS19に進む。~~

【0632】

また、ステップS17の処理に進むと、セキュリティモジュール13は、自己が保持するリストを用いて光ディスク記録再生装置100のID_Bの検証を行った後、ステップS19に進む。

【0633】

また、ステップS18の処理に進むと、セキュリティモジュール13は、光ディスク記録再生装置100からリストを受信し、そのバージョンナンバー(Rev V_B, Reg V_B)の検証と、当該リストを用いた光ディスク記録再生装置100のID_Bの検証と、センタTCの署名TCSigの検証を行った後、ステップS19に進む。

【0634】

ステップS19の処理に進むと、セキュリティモジュール13は、光ディスク記録再生装置から記録又は再生の何れの処理が要求されているのか判定する。

【0635】

当該ステップS19にて記録の処理が要求されていると判定した場合、セキュリティモジュール13は、ステップS20の処理として、光ディスク記録再生装

置がセッション鍵 K_{se} にて暗号鍵 K_{co} を暗号化した値 $E_{nc}(K_{se}, K_{co})$ を受信して復号し、次に、その復号により得られた暗号鍵 K_{co} を自己が保持するストレージ鍵 K_{st} で暗号化した値 $E_{nc}(K_{st}, K_{co})$ を生成して光ディスク記録再生装置に送信する。その後、光ディスク記録再生装置において上記暗号鍵 K_{co} にて暗号化されたコンテンツデータ $E_{nc}(K_{se}, K_{co})$ が、光ディスク 1 2 に記録されることになる。

【0636】

一方、ステップ S 1 9 にて再生の処理が要求されていると判定した場合、セキュリティモジュール 1 3 は、ステップ S 2 1 の処理として、ストレージ鍵 K_{st} にて暗号鍵 K_{co} が暗号化され例えば光ディスク 1 2 のデータ記録領域等に記録されている値 $E_{nc}(K_{st}, K_{co})$ を読み出して復号し、その復号により得られた暗号鍵 K_{co} をセッション鍵 K_{se} にて暗号化した値 $E_{nc}(K_{se}, K_{co})$ を生成して光ディスク記録再生装置に送信する。その後、上記暗号鍵 K_{co} にて暗号化されているコンテンツデータ $E_{nc}(K_{se}, K_{co})$ は、光ディスク 1 2 から再生されて光ディスク記録再生装置に送られることになる。

【0637】

図 8 3 には、前記メディアタイプ IM 3 に相当するメモリ情報記録媒体 6 0 のセキュリティモジュール 6 3 における処理の流れを示す。

【0638】

この図 8 3 において、セキュリティモジュール 6 3 は、ステップ S 3 1 として、前述したように、メモリ記録再生装置が発生した乱数 R_B の受信と、前記 $V_A = K_A \cdot G$ の計算、乱数 R_A の発生、デジタル署名を行い Sig_A 計算、 $Cert_A$, R_A , R_B , V_A , $RevV_A$, $RegV_A$, Sig_A をメモリ記録再生装置に送信する。

【0639】

次に、セキュリティモジュール 6 3 は、ステップ S 3 2 として、メモリ記録再生装置から送信されてきた $Cert_B$, R_B , R_A , V_B , $RevV_B$, $RegV_B$, Sig_B 受信、 $Cert_B$ の検証、 Sig_B の検証、セッション鍵 K_{se} の計算を行う。

【0640】

次に、セキュリティモジュール 6 3 は、ステップ S 3 3 として、例えばリスト

のバージョンナンバーが「0」か否かにより、相手方のメモリ記録再生装置のデバイスタイプを判定する。このステップS33の判定において、例えばリストのバージョンナンバーが「0」となっており、前記デバイスタイプDev3（メモリ記録再生装置400）であると判定した場合、セキュリティモジュール63の処理は、ステップS34に進む。一方、ステップS33の判定において、リストのバージョンナンバーが「0」でなく、前記デバイスタイプDev4（メモリ記録再生装置200）であると判定した場合、セキュリティモジュール63の処理は、ステップS35に進む。

【0641】

ステップS34の処理に進むと、セキュリティモジュール63は、メモリ部22のデータ記録領域に格納しているリストを用いてメモリ記録再生装置400のID_Bを検証し、その検証をパスしたとき、上記リストをメモリ記録再生装置400に送信した後、ステップS39の処理に進む。

【0642】

また、ステップS35の処理に進むと、セキュリティモジュール63は、メモリ部22のデータ記録領域に格納しているリストのバージョンが、メモリ記録再生装置200が保持するリストのバージョンナンバーよりも大きい（ $A > B$ ）か、或いは等しいか（ $A = B$ ）、或いは小さいか（ $A < B$ ）の判定を行う。このステップS35の判定において、 $A > B$ であると判定した場合、セキュリティモジュール63の処理はステップS36に進み、 $A = B$ であると判定した場合、セキュリティモジュール63の処理はステップS37に進み、 $A > B$ であると判定した場合、セキュリティモジュール63の処理はステップS38に進む。

【0643】

ステップS36の処理に進むと、セキュリティモジュール63は、メモリ部22のデータ記録領域に記録されていたリストを読み出し、そのバージョンナンバー（RevV_A, RegV_A）の検証と、当該リストを用いたメモリ記録再生装置200のID_Bの検証と、センタTCの署名TCSigの検証を行い、さらに当該リストをメモリ記録再生装置200に送信した後、ステップS39に進む。

【0644】

また、ステップS37の処理に進むと、セキュリティモジュール63は、メモリ部22のデータ記録領域に記録されていたリストを読み出し、そのバージョンナンバー ($RevV_A$, $RegV_A$) の検証と、当該リストを用いたメモリ記録再生装置200のID_Bの検証と、センタTCの署名TCSigの検証を行った後、ステップS39に進む。

【0645】

また、ステップS38の処理に進むと、セキュリティモジュール63は、メモリ記録再生装置200からリストを受信し、そのバージョンナンバー ($RevV_B$, $RegV_B$) の検証と、当該リストを用いたメモリ記録再生装置200のID_Bの検証と、~~センタTCの署名TCSigの検証を行い、さらに、そのリストをメモリ部22に書き込んで更新した後、~~ステップS39に進む。

【0646】

ステップS39の処理に進むと、セキュリティモジュール63は、メモリ記録再生装置から記録又は再生の何れの処理が要求されているのか判定する。

【0647】

当該ステップS39にて記録の処理が要求されていると判定した場合、セキュリティモジュール63は、ステップS40の処理として、メモリ記録再生装置がセッション鍵K_{se}にて暗号鍵K_{co}を暗号化した値Enc (K_{se}, K_{co}) を受信して復号し、次に、その復号により得られた暗号鍵K_{co}を自己が保持するストレージ鍵K_{st}で暗号化した値Enc (K_{st}, K_{co}) を生成してメモリ記録再生装置に送信する。その後、セキュリティモジュール63は、上記メモリ記録再生装置において上記暗号鍵K_{co}にて暗号化されたコンテンツデータEnc (K_{se}, K_{co}) を受信し、メモリ部22に記録する。

【0648】

一方、ステップS39にて再生の処理が要求されていると判定した場合、セキュリティモジュール63は、ステップS41の処理として、ストレージ鍵K_{st}にて暗号鍵K_{co}が暗号化され例えばメモリ部22のデータ記録領域等に記録されている値Enc (K_{st}, K_{co}) を読み出して復号し、その復号により得られた暗号鍵K

coをセッション鍵 K_{se} にて暗号化した値 $E_{nc}(K_{se}, K_{co})$ を生成してメモリ記録再生装置に送信する。その後、セキュリティモジュール63は、メモリ部22から上記暗号鍵 K_{co} にて暗号化されているコンテンツデータ $E_{nc}(K_{se}, K_{co})$ を読み出し、メモリ記録再生装置に送る。

【0649】

図84には、前記メディアタイプIM4に相当するメモリ情報記録媒体20のセキュリティモジュール23における処理の流れを示す。

【0650】

この図84において、セキュリティモジュール23は、ステップS51として、前述したように、メモリ記録再生装置が発生した乱数 R_B の受信と、前記 $V_A = K_A \cdot G$ の計算、乱数 R_A の発生、デジタル署名を行い Sig_A 計算、 $Cert_A$ 、 R_A 、 R_B 、 V_A 、 $RevV_A$ 、 $RegV_A$ 、 Sig_A をメモリ記録再生装置に送信する。

【0651】

次に、セキュリティモジュール23は、ステップS52として、メモリ記録再生装置から送信されてきた $Cert_B$ 、 R_B 、 R_A 、 V_B 、 $RevV_B$ 、 $RegV_B$ 、 Sig_B 受信、 $Cert_B$ の検証、 Sig_B の検証、セッション鍵 K_{se} の計算を行う。

【0652】

次に、セキュリティモジュール23は、ステップS53として、例えばリストのバージョンナンバーが「0」か否かにより、相手方のメモリ記録再生装置のデバイスタイプを判定する。このステップS53の判定において、例えばリストのバージョンナンバーが「0」となっており、前記デバイスタイプDev3（メモリ記録再生装置400）であると判定した場合、セキュリティモジュール23の処理は、ステップS54に進む。一方、ステップS53の判定において、リストのバージョンナンバーが「0」でなく、前記デバイスタイプDev4（メモリ記録再生装置200）であると判定した場合、セキュリティモジュール23の処理は、ステップS55に進む。

【0653】

ステップS54の処理に進むと、セキュリティモジュール23は、不揮発性メモリ44に格納しているリストを用いてメモリ記録再生装置400のID_Bを検

証し、その検証をパスしたとき、上記リストをメモリ記録再生装置 4 0 0 に送信した後、ステップ S 5 9 の処理に進む。

【0 6 5 4】

また、ステップ S 5 5 の処理に進むと、セキュリティモジュール 2 3 は、不揮発性メモリ 4 4 に格納しているリストのバージョンが、メモリ記録再生装置 2 0 0 が保持するリストのバージョンナンバーよりも大きい ($A > B$) か、或いは等しいか ($A = B$)、或いは小さいか ($A < B$) の判定を行う。このステップ S 5 5 の判定において、 $A > B$ であると判定した場合、セキュリティモジュール 2 3 の処理はステップ S 5 6 に進み、 $A = B$ であると判定した場合、セキュリティモジュール 2 3 の処理はステップ S 5 7 に進み、 $A < B$ であると判定した場合、セキュリティモジュール 2 3 の処理はステップ S 5 8 に進む。

【0 6 5 5】

ステップ S 5 6 の処理に進むと、セキュリティモジュール 2 3 は、自己が保持するリストを用いてメモリ記録再生装置 2 0 0 の ID_B の検証を行い、そのリストをメモリ記録再生装置 1 0 0 に送信した後、ステップ S 5 9 に進む。

【0 6 5 6】

また、ステップ S 5 7 の処理に進むと、セキュリティモジュール 2 3 は、自己が保持するリストを用いてメモリ記録再生装置 2 0 0 の ID_B の検証を行った後、ステップ S 5 9 に進む。

【0 6 5 7】

また、ステップ S 5 8 の処理に進むと、セキュリティモジュール 2 3 は、メモリ記録再生装置 2 0 0 からリストを受信し、そのバージョンナンバー ($RevV_B$, $RegV_B$) の検証と、当該リストを用いたメモリ記録再生装置 2 0 0 の ID_B の検証と、センタ TC の署名 $TC\text{Sig}$ の検証を行った後、ステップ S 5 9 に進む。

【0 6 5 8】

ステップ S 5 9 の処理に進むと、セキュリティモジュール 2 3 は、メモリ記録再生装置から記録又は再生の何れの処理が要求されているのか判定する。

【0 6 5 9】

当該ステップ S 5 9 にて記録の処理が要求されていると判定した場合、セキュ

リティモジュール 2 3 は、ステップ S 6 0 の処理として、メモリ記録再生装置がセッション鍵 K_{se} にて暗号鍵 K_{co} を暗号化した値 $E_{nc}(K_{se}, K_{co})$ を受信して復号し、次に、その復号により得られた暗号鍵 K_{co} を自己が保持するストレージ鍵 K_{st} で暗号化した値 $E_{nc}(K_{st}, K_{co})$ を生成して光ディスク記録再生装置に送信する。その後、セキュリティモジュール 2 3 は、上記メモリ記録再生装置において上記暗号鍵 K_{co} にて暗号化されたコンテンツデータ $E_{nc}(K_{se}, K_{co})$ を受信し、メモリ部 2 2 に記録する。

【0 6 6 0】

一方、ステップ S 5 9 にて再生の処理が要求されていると判定した場合、セキュリティモジュール 2 3 は、ステップ S 6 1 の処理として、ストレージ鍵 K_{st} にて暗号鍵 K_{co} が暗号化され例えばメモリ部 2 2 のデータ記録領域等に記録されている値 $E_{nc}(K_{st}, K_{co})$ を読み出して復号し、その復号により得られた暗号鍵 K_{co} をセッション鍵 K_{se} にて暗号化した値 $E_{nc}(K_{se}, K_{co})$ を生成してメモリ記録再生装置に送信する。その後、上記暗号鍵 K_{co} にて暗号化されているコンテンツデータ $E_{nc}(K_{se}, K_{co})$ は、メモリ部 2 2 から再生されてメモリ記録再生装置に送られることになる。

【0 6 6 1】

次に、前記デバイスタイプ $Dev1 \sim Dev4$ に相当する各光ディスク記録再生装置、メモリ記録再生装置における処理の流れを示す。なお、デバイスタイプ $Dev1$ に相当する光ディスク記録再生装置 3 0 0 とデバイスタイプ $Dev3$ に相当するメモリ記録再生装置 4 0 0 の処理の流れは略々同じであり、また、デバイスタイプ $Dev2$ に相当する光ディスク記録再生装置 1 0 0 とデバイスタイプ $Dev4$ に相当するメモリ記録再生装置 2 0 0 の処理の流れは略々同じであるため、以下の説明では、デバイスタイプ $Dev1$ 及び $Dev3$ での処理と、デバイスタイプ $Dev2$ 及び $Dev4$ での処理を、それぞれ纏めて説明する。

【0 6 6 2】

図 8 5 には、デバイスタイプ $Dev1$ 及び $Dev3$ の記録再生装置の処理の流れを示す。

【0 6 6 3】

この図 8 5 において、記録再生装置は、ステップ S 7 1 の処理として、先ず、乱数 R_B を発生して情報記録媒体に送信する。

【0 6 6 4】

次に、記録再生装置は、ステップ S 7 2 の処理として、情報記録媒体から送信されてきた $Cert_A$, R_A , R_B , V_A , $RevV_A$, $RegV_A$, Sig_A を受信する。またお、メディア記録再生装置に送信し、 $Cert_A$ の検証、 Sig_A の検証、前記 $V_B = K_B \cdot G$ の計算を行った後、情報記録媒体に対して、 $Cert_B$, R_B , R_A , V_B , $RevV_B$, $RegV_B$, Sig_B を送信する。なお、このときバージョンナンバー $RevV_B$, $RegV_B$ は「0」となる。

【0 6 6 5】

次に、記録再生装置は、ステップ S 7 3 の処理として、セッション鍵 K_{se} の計算を行う。

【0 6 6 6】

次に、記録再生装置は、ステップ S 7 4 として、情報記録媒体のメディアタイプが、IM 1 か或いはそれ以外 (IM 2, IM 3, IM 4) か否かの判定を行う。当該ステップ S 7 4 の判定において、情報記録媒体がメディアタイプ IM 1 であると判定した場合、記録再生装置の処理はステップ S 7 5 に進み、情報記録媒体がメディアタイプ IM 1 でない (メディアタイプ IM 2, IM 3, IM 4) であると判定した場合、記録再生装置の処理はステップ S 7 6 に進む。

【0 6 6 7】

ステップ S 7 5 の処理に進むと、記録再生装置は、メディアタイプ IM 1 の光ディスク情報記録媒体 5 0 の光ディスク 1 2 からリボケーションリスト/レジストレーションリストを読み出し、そのリストのバージョンナンバー ($RevV_A$, $RegV_A$) の検証と、そのリストを用いた光ディスク情報記録媒体 5 0 の ID_A の検証と、センタ TC の署名 TC_{Sig} の検証を行い、そのリストを光ディスク情報記録媒体 5 0 のセキュリティモジュール 5 3 に送信した後、ステップ S 7 7 に進む。

【0668】

また、ステップS76の処理に進むと、記録再生装置は、メディアタイプIM1でないメディアタイプ(IM2～IM4)の情報記録媒体からリボケーションリスト/レジストレーションリストを読み出し、そのリストのバージョンナンバー($RevV_A$, $RegV_A$)の検証と、そのリストを用いた情報記録媒体のID_Aの検証と、センタTCの署名TCSigの検証を行った後、ステップS77に進む。

【0669】

ステップS77の処理に進むと、記録再生装置は、情報記録媒体に対してデータの記録を行うのか、或いは情報記録媒体からデータの再生を行うのか判定する。

【0670】

当該ステップS77にて記録の処理を行うと判定した場合、記録再生装置は、ステップS78の処理として、再度、メディアタイプが、IM1, IM2(すなわち光ディスク情報記録媒体)であるか、或いはIM3, IM4(すなわちメモリ情報記録媒体)であるかの判定を行う。当該ステップS78の判定において、情報記録媒体がメディアタイプIM1, IM2であると判定した場合、記録再生装置の処理はステップS80に進み、情報記録媒体がメディアタイプIM3, IM4であると判定した場合、記録再生装置の処理はステップS81に進む。

【0671】

また、上記ステップS77にて再生の処理を行うと判定した場合、記録再生装置は、ステップS79の処理として、再度、メディアタイプが、IM1, IM2(光ディスク情報記録媒体)であるか、或いはIM3, IM4(メモリ情報記録媒体)であるかの判定を行う。当該ステップS79の判定において、情報記録媒体がメディアタイプIM1, IM2であると判定した場合、記録再生装置の処理はステップS82に進み、情報記録媒体がメディアタイプIM3, IM4であると判定した場合、記録再生装置の処理はステップS83に進む。

【0672】

上記ステップS80の処理に進むと、記録再生装置は、セッション鍵K_{se}にて暗号鍵K_{co}を暗号化した値Enc(K_{se}, K_{co})を送信し、それに対応して情報記録

媒体がストレージ鍵 K_{st} で暗号鍵 K_{co} を暗号化して送信してきた値 $E_{nc}(K_{st}, K_{co})$ を受信した後、ストレージ鍵 K_{st} で暗号鍵 K_{co} を暗号化した値 $E_{nc}(K_{st}, K_{co})$ と暗号鍵 K_{co} でコンテンツデータを暗号化したデータ $E_{nc}(K_{co}, data)$ を情報記録媒体に書き込む。

【0673】

また、ステップ S 8 1 の処理に進むと、記録再生装置は、セッション鍵 K_{se} にて暗号鍵 K_{co} を暗号化した値 $E_{nc}(K_{se}, K_{co})$ を送信した後、暗号鍵 K_{co} でコンテンツデータを暗号化したデータ $E_{nc}(K_{co}, data)$ を情報記録媒体に書き込む。

【0674】

また、ステップ S 8 2 の処理に進むと、記録再生装置は、ストレージ鍵 K_{st} にて暗号鍵 K_{co} が暗号化された値 $E_{nc}(K_{st}, K_{co})$ を情報記録媒体から読み出し、その値 $E_{nc}(K_{st}, K_{co})$ を情報記録媒体のセキュリティモジュールに送信し、情報記録媒体が値 $E_{nc}(K_{st}, K_{co})$ をストレージ鍵 K_{st} で復号し、さらにその暗号鍵 K_{co} をセッション鍵 K_{se} で暗号化した値 $E_{nc}(K_{se}, K_{co})$ を受信した後、当該暗号鍵 K_{co} で暗号化されているコンテンツデータ $E_{nc}(K_{co}, data)$ を情報記録媒体から読み出す。

【0675】

また、ステップ S 8 3 の処理に進むと、記録再生装置は、セッション鍵 K_{se} にて暗号鍵 K_{co} を暗号化した値 $E_{nc}(K_{se}, K_{co})$ を情報記録媒体から受信した後、当該暗号鍵 K_{co} で暗号化されているコンテンツデータ $E_{nc}(K_{co}, data)$ を情報記録媒体から読み出す。

【0676】

図 8 6 及び図 8 7 には、デバイスタイプ $Dev 2$ 及び $Dev 3$ の記録再生装置の処理の流れを示す。なお、図 8 6 と図 8 7 は、本来は 1 つの図面上に描く幕であるが、紙面の都合で 2 つの図に分けている。

【0677】

この図 8 6 において、記録再生装置は、ステップ S 9 1 の処理として、まず、乱数 R_B を発生して情報記録媒体に送信する。

【0678】

次に、記録再生装置は、ステップS92の処理として、情報記録媒体から送信されてきた $Cert_A$, R_A , R_B , V_A , $RevV_A$, $RegV_A$, Sig_A を受信する。またお、メディア記録再生装置に送信し、 $Cert_A$ の検証、 Sig_A の検証、前記 $V_B = K_B \cdot G$ の計算を行った後、情報記録媒体に対して、 $Cert_B$, R_B , R_A , V_B , $RevV_B$, $RegV_B$, Sig_B を送信する。

【0679】

次に、記録再生装置は、ステップS93の処理として、セッション鍵 K_{se} の計算を行う。

【0680】

次に、記録再生装置は、ステップS94として、情報記録媒体のメディアタイプが、IM1か或いはそれ以外(IM2, IM3, IM4)か否かの判定を行う。当該ステップS94の判定において、情報記録媒体がメディアタイプIM1であると判定した場合、記録再生装置の処理はステップS95に進み、情報記録媒体がメディアタイプIM1でない(メディアタイプIM2, IM3, IM4)であると判定した場合、記録再生装置の処理はステップS96に進む。

【0681】

ステップS95の処理に進むと、記録再生装置は、上記 $RevV_A$, $RegV_A$ と、 $RevV_B$, $RegV_B$ からバージョンの新しさの判断を行う。すなわち記録再生装置は、そのリストのバージョンが、記録再生装置の保持するバージョンナンバーよりも大きい($A > B$)か、或いは等しいか($A = B$)、或いは小さいか($A < B$)の判定を行う。このステップS95の判定において、 $A > B$ であると判定した場合、記録再生装置の処理はステップS97に進み、 $A = B$ であると判定した場合、記録再生装置の処理はステップS98に進み、 $A < B$ であると判定した場合、記録再生装置の処理はステップS99に進む。

【0682】

ステップS97の処理に進むと、記録再生装置は、メディアタイプIM1の光ディスク情報記録媒体50の光ディスク12からリボケーションリスト/レジストレーションリストを読み出し、そのリストのバージョンナンバー($RevV_A$,

RegV_A) の検証と、そのリストを用いた光ディスク情報記録媒体 5 0 の ID_A の検証と、センタ TC の署名 TC Sig の検証を行い、そのリストを光ディスク情報記録媒体 5 0 のセキュリティモジュール 5 3 に送信した後、図 8 7 のステップ S 1 1 0 の処理に進む。

【0 6 8 3】

また、ステップ S 9 8 の処理に進むと、記録再生装置は、自己が保持するリストを用いて情報記録媒体 ID_A の検証を行い、当該リストを情報記録媒体の送信した後、図 8 7 のステップ S 1 1 0 の処理に進む。

【0 6 8 4】

また、ステップ S 9 9 の処理に進むと、記録再生装置は、自己が保持するリストを用いて情報記録媒体 ID_A の検証を行い、当該リストを情報記録媒体の送信する。さらに、記録再生装置は、ステップ S 1 0 3 で、上記情報記録媒体に対して当該リストを書き込ませ（更新）した後、図 8 7 のステップ S 1 1 0 の処理に進む。

【0 6 8 5】

一方、上記ステップ S 9 6 の処理に進むと、記録再生装置は、上記 RevV_A, RegV_A と、RevV_B, RegV_B からバージョンの新しさの判断を行う。すなわち記録再生装置は、そのリストのバージョンが、記録再生装置の保持するバージョンナンバーよりも大きい ($A > B$) か、或いは等しいか ($A = B$)、或いは小さいか ($A < B$) の判定を行う。このステップ S 9 6 の判定において、 $A > B$ であると判定した場合、記録再生装置の処理はステップ S 1 0 0 に進み、 $A = B$ であると判定した場合、記録再生装置の処理はステップ S 1 0 1 に進み、 $A < B$ であると判定した場合、記録再生装置の処理はステップ S 1 0 2 に進む。

【0 6 8 6】

ステップ S 1 0 0 の処理に進むと、記録再生装置は、メディアタイプ IM 2 ~ IM 4 の情報記録媒体からリボケーションリスト／レジストレーションリストを読み出し、そのリストのバージョンナンバー (RevV_A, RegV_A) の検証と、そのリストを用いた情報記録媒体の ID_A の検証と、センタ TC の署名 TC Sig の検証を行い、その後、図 8 7 のステップ S 1 1 0 の処理に進む。

【0687】

また、ステップS101の処理に進むと、記録再生装置は、自己が保持するリストを用いて情報記録媒体ID_Aの検証を行った後、図87のステップS110の処理に進む。

【0688】

また、ステップS102の処理に進むと、記録再生装置は、自己が保持するリストを用いて情報記録媒体ID_Aの検証を行い、当該リストを情報記録媒体に送信した後、図87のステップS110の処理に進む。

【0689】

図87のステップS110の処理に進むと、記録再生装置は、情報記録媒体に対してデータの記録を行うのか、或いは情報記録媒体からデータの再生を行うのか判定する。

【0690】

当該ステップS110にて記録の処理を行うと判定した場合、記録再生装置は、ステップS111の処理として、再度、メディアタイプが、IM1, IM2（光ディスク情報記録媒体）であるか、或いはIM3, IM4（メモリ情報記録媒体）であるかの判定を行う。当該ステップS111の判定において、情報記録媒体がメディアタイプIM1, IM2であると判定した場合、記録再生装置の処理はステップS113に進み、情報記録媒体がメディアタイプIM3, IM4であると判定した場合、記録再生装置の処理はステップS114に進む。

【0691】

また、上記ステップS110にて再生の処理を行うと判定した場合、記録再生装置は、ステップS112の処理として、再度、メディアタイプが、IM1, IM2（光ディスク情報記録媒体）であるか、或いはIM3, IM4（メモリ情報記録媒体）であるかの判定を行う。当該ステップS112の判定において、情報記録媒体がメディアタイプIM1, IM2であると判定した場合、記録再生装置の処理はステップS115に進み、情報記録媒体がメディアタイプIM3, IM4であると判定した場合、記録再生装置の処理はステップS116に進む。

【0692】

上記ステップ S 1 1 3 の処理に進むと、記録再生装置は、セッション鍵 K_{se} にて暗号鍵 K_{co} を暗号化した値 $E_{nc}(K_{se}, K_{co})$ を送信し、それに対応して情報記録媒体がストレージ鍵 K_{st} で暗号鍵 K_{co} を暗号化して送信してきた値 $E_{nc}(K_{st}, K_{co})$ を受信した後、ストレージ鍵 K_{st} で暗号鍵 K_{co} を暗号化した値 $E_{nc}(K_{st}, K_{co})$ と暗号鍵 K_{co} でコンテンツデータを暗号化したデータ $E_{nc}(K_{co}, data)$ を情報記録媒体に書き込む。

【0693】

また、ステップ S 1 1 4 の処理に進むと、記録再生装置は、セッション鍵 K_{se} にて暗号鍵 K_{co} を暗号化した値 $E_{nc}(K_{se}, K_{co})$ を送信した後、暗号鍵 K_{co} でコンテンツデータを暗号化したデータ $E_{nc}(K_{co}, data)$ を情報記録媒体に書き込む。

【0694】

また、ステップ S 1 1 5 の処理に進むと、記録再生装置は、ストレージ鍵 K_{st} にて暗号鍵 K_{co} が暗号化された値 $E_{nc}(K_{st}, K_{co})$ を情報記録媒体から読み出し、その値 $E_{nc}(K_{st}, K_{co})$ を情報記録媒体のセキュリティモジュールに送信し、情報記録媒体が値 $E_{nc}(K_{st}, K_{co})$ をストレージ鍵 K_{st} で復号し、さらにその暗号鍵 K_{co} をセッション鍵 K_{se} で暗号化した値 $E_{nc}(K_{se}, K_{co})$ を受信した後、当該暗号鍵 K_{co} で暗号化されているコンテンツデータ $E_{nc}(K_{co}, data)$ を情報記録媒体から読み出す。

【0695】

また、ステップ S 1 1 6 の処理に進むと、記録再生装置は、セッション鍵 K_{se} にて暗号鍵 K_{co} を暗号化した値 $E_{nc}(K_{se}, K_{co})$ を情報記録媒体から受信した後、当該暗号鍵 K_{co} で暗号化されているコンテンツデータ $E_{nc}(K_{co}, data)$ を情報記録媒体から読み出す。

【0696】

なお、上述した実施の形態では、本発明を適用した情報記録媒体として光ディスク記録媒体とメモリ情報記録媒体の例を提示したが、情報記録媒体はこれに限るものではなく、磁気ディスクや磁気テープ、光磁気ディスク、バッテリーバッ

クアップされた揮発性メモリなどでもよい。

【0697】

次に、上述した本発明の情報記録媒体を製造する本発明の記録媒体製造装置及び方法について説明する。

【0698】

以下に、本発明の情報記録媒体として前述した実施の形態のメディアタイプIM1～IM4の各情報記録媒体を例に挙げ、それら各メディアタイプIM1～IM4の情報記録媒体をそれぞれ製造する記録媒体製造装置について説明を行う。

【0699】

図88には、メディアタイプIM1の光ディスク情報記録媒体50を製造すると共に、当該光ディスク情報記録媒体50に対して最新のリストを記録する記録媒体製造装置である光ディスク製造装置500の概略構成を示す。なお、記録する最新のリストは、リボケーションリスト又はレジストレーションリストの一方、或いは、リボケーションリスト及びレジストレーションリストの両方の何れであっても良い。

【0700】

この図88に示す光ディスク製造装置500は、図示しない組立工程により既に組み立てられている光ディスク情報記録媒体50に対して、リストを記録する。但し、メディアタイプIM1である光ディスク情報記録媒体50は、前述したようにセキュリティモジュール53がリストを格納するための不揮発性メモリを備えていないか、或いは不揮発性メモリがリストを格納するのに十分な記憶容量を備えていないため、当該光ディスク製造装置500は、光ディスク情報記録媒体50のコンテンツデータ記録用の領域に上記リストを記録する。

【0701】

このため、当該光ディスク製造装置500は、光ディスク情報記録媒体50のカートリッジ11内の光ディスク12を回転させるスピンドルモータ501と、光ディスク12のデータ記録領域に情報を少なくとも書き込み可能な光学ヘッド502と、スピンドルモータ501や光学ヘッド502のサーボ回路503と、これらを制御する制御部505等を備えている。

【 0 7 0 2 】

さらに、光ディスク製造装置 5 0 0 は、光ディスク情報記録媒体 5 0 の I D、秘密鍵、公開鍵証明書、当該媒体 5 0 の製造時点における最新のリスト及びそのバージョンナンバーを予め格納している鍵・リスト記録媒体 5 0 7 と、そのドライブ部 6 0 6 と、光ディスク情報記録媒体 5 0 のセキュリティモジュール 5 3 との間で情報の授受を行うインターフェース部 5 0 8 とを備えている。なお、図 8 8 の構成では、鍵・リスト記録媒体 5 0 7 及びドライブ部 5 0 6 は、当該光ディスク製造装置 5 0 0 に内蔵されている例を挙げているが、当該鍵・リスト記録媒体 5 0 7 及びドライブ部 5 0 6 は外付けの媒体及びドライブであってもよい。上記 I D、秘密鍵、公開鍵証明書、最新のリスト及びバージョンナンバーは、例えば図示しない鍵発行センタにより発行されるものであり、上記内蔵或いは外付けの鍵・リスト記録媒体に予め格納されている。

【 0 7 0 3 】

上記鍵・リスト記録媒体 5 0 7 に格納されている情報は、制御部 5 0 5 の制御の下、ドライブ部 5 0 6 により読み取られ、当該読み取られた情報のうち、上記 I D、秘密鍵、公開鍵証明書、バージョンナンバーについてはインターフェース部 5 0 8 から光ディスク情報記録媒体 5 0 のセキュリティモジュール 5 3 に送られて記憶され、上記最新のリストは光学ヘッド 5 0 2 にて光ディスク 1 2 のデータ記録領域に記録される。

【 0 7 0 4 】

また、I D、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーは、上述したように内蔵或いは外付けの鍵・リスト記録媒体に予め格納されているものを読み取るだけでなく、例えば鍵発行センタより送られてきたものを外部インターフェース部 5 0 9 を介して直接に入手することも可能である。このように、外部インターフェース部 5 0 9 を介して I D、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーを入手するようにした場合、当該外部インターフェース部 5 0 9 を介した I D、秘密鍵、公開鍵証明書、バージョンナンバーは制御部 5 0 5 からインターフェース部 5 0 8 に直接送られて光ディスク情報記録媒体 5 0 のセキュリティモジュール 5 3 に記憶され、上記最新のリストは制

御部 505 から光学ヘッド 502 に直接送られて光ディスク 12 のデータ記録領域に記録されることになる。

【0705】

図 89 には、本発明の記録媒体製造方法として、上記メディアタイプ IM1 の光ディスク情報記録媒体 50 を製造すると共に、当該光ディスク情報記録媒体 50 に対して最新のリストを記録する光ディスク製造方法における製造工程の流れを示す。

【0706】

図 89 において、光ディスク製造方法では、先ず、ステップ S200 の製造工程として、図示しない組立工程によりメディアタイプ IM1 の光ディスク情報記録媒体 50 が組み立てられる。

【0707】

次に、光ディスク製造方法では、ステップ S201 の製造工程として、図 88 の光ディスク製造装置 500 により、前記 ID、秘密鍵、公開鍵証明書、バージョンナンバーを、メディアタイプ IM1 である光ディスク情報記録媒体 50 のセキュリティモジュール 53 内に設けられている不揮発性の鍵メモリ 36 に書き込む。

【0708】

次に、光ディスク製造方法では、ステップ S202 の製造工程として、図 88 の光ディスク製造装置 500 により、最新のリストを光ディスク 12 のコンテンツデータ記録用の領域に書き込む。

【0709】

以上により、光ディスク情報記録媒体 50 は、最新版のリストをデータ記録領域に記録した状態で製造工場から出荷されることになる。

【0710】

図 90 には、メディアタイプ IM2 の光ディスク情報記録媒体 10 を製造すると共に、当該光ディスク情報記録媒体 10 に対して最新のリストを記録する記録媒体製造装置である光ディスク製造装置 510 の概略構成を示す。なお、記録する最新のリストは、リボケーションリスト又はレジストレーションリストの一方

、或いは、リボケーションリスト及びレジストレーションリストの両方の何れであっても良い。

【0711】

この図90に示す光ディスク製造装置510は、図示しない組立工程により既に組み立てられている光ディスク情報記録媒体10に対して、リストを記録する。但し、メディアタイプIM2である光ディスク情報記録媒体10は、前述したようにセキュリティモジュール13がリストを格納するための十分な記憶容量を有する不揮発性メモリ(34)を備えているため、当該光ディスク製造装置510は、光ディスク情報記録媒体10のセキュリティモジュール13の不揮発性メモリに上記リストを記録する。

【0712】

このため、当該光ディスク製造装置510は、少なくとも、光ディスク情報記録媒体10のセキュリティモジュール13にリストを送信するためのインターフェース部518と、各部を制御する制御部515等を備えている。なお、図90の例では、図58の例のようにスピンドルモータや光学ヘッド等を備えていない構成を挙げているが、光ディスク製造装置510はもちろんそれらを備えていてもよい。

【0713】

さらに、光ディスク製造装置510は、光ディスク情報記録媒体10のID、秘密鍵、公開鍵証明書、当該媒体10の製造時点における最新のリスト及びそのバージョンナンバーを予め格納している鍵・リスト記録媒体517とそのドライブ部516も備えている。なお、図90の構成では、鍵・リスト記録媒体517及びドライブ部516は、当該光ディスク製造装置510に内蔵されている例を挙げているが、当該鍵・リスト記録媒体517及びドライブ部516は外付けの媒体及びドライブであってもよい。上記ID、秘密鍵、公開鍵証明書、最新のリスト及びバージョンナンバーは、図示しない鍵発行センタにより発行されるものであり、上記内蔵或いは外付けの鍵・リスト記録媒体に予め格納されている。

【0714】

上記鍵・リスト記録媒体517に格納されている情報は、制御部515の制御

の元、ドライブ部 516 により読み取られ、インターフェース部 518 から光ディスク情報記録媒体 10 のセキュリティモジュール 13 に送られて不揮発性メモリ (34) に記憶される。

【0715】

また、この図 90 の例でも前記図 88 の場合と同様に、ID、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーは、上述した内蔵或いは外付けの鍵・リスト記録媒体に予め格納されているものを読み取るだけでなく、鍵発行センタより送られてきたものを外部インターフェース部 519 を介して直接に入手することも可能である。外部インターフェース部 519 を介して ID、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーを入手するように

した場合、当該外部インターフェース部 519 を介した ID、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーは、制御部 515 からインターフェース部 518 に直接送られて光ディスク情報記録媒体 10 のセキュリティモジュール 13 に送られて不揮発性メモリ 34 に記録されることになる。

【0716】

図 91 には、本発明の記録媒体製造方法として、上記メディアタイプ IM2 の光ディスク情報記録媒体 10 を製造すると共に、当該光ディスク情報記録媒体 10 に対して最新のリストを記録する光ディスク製造方法における製造工程の流れを示す。

【0717】

図 91 において、光ディスク製造方法では、先ず、ステップ S210 の製造工程として、図示しない組立工程によりメディアタイプ IM2 の光ディスク情報記録媒体 10 が組み立てられる。

【0718】

次に、光ディスク製造方法では、ステップ S211 の製造工程として、図 90 の光ディスク製造装置 510 により、前記 ID、秘密鍵、公開鍵証明書、バージョンナンバーを、メディアタイプ IM2 である光ディスク情報記録媒体 10 のセキュリティモジュール 13 内に設けられている不揮発性メモリ 34 に書き込む。

【0719】

次に、光ディスク製造方法では、ステップS212の製造工程として、図90の光ディスク製造装置510により、最新のリストを光ディスク情報記録媒体10のセキュリティモジュール13内に設けられている不揮発性メモリ34に書き込む。

【0720】

以上により、光ディスク記録再生装置10は、セキュリティモジュール13に最新版のリストを記録した状態で製造工場から出荷されることになる。

【0721】

図92には、メディアタイプIM3のメモリ情報記録媒体60を製造すると共に、~~当該メモリ情報記録媒体60に対して最新のリストを記録する記録媒体製造~~装置であるメモリ製造装置600の概略構成を示す。なお、記録する最新のリストは、リボケーションリスト又はレジストレーションリストの一方、或いは、リボケーションリスト及びレジストレーションリストの両方の何れであっても良い。

【0722】

この図92に示すメモリ製造装置600は、図示しない組立工程により既に組み立てられているメモリ情報記録媒体60に対して、リストを記録する。但し、メディアタイプIM3であるメモリ情報記録媒体60は、前述したようにセキュリティモジュール63がリストを格納するための不揮発性メモリを備えていないか、或いは不揮発性メモリがリストを格納するのに十分な記憶容量を備えていないため、当該メモリ製造装置600は、メモリ情報記録媒体60のメモリ部22のコンテンツデータ記録用の領域に上記リストを記録する。

【0723】

このため、当該メモリ製造装置600は、少なくとも、メモリ情報記録媒体60に信号を送信するためのインターフェース部608と、メモリ情報記録媒体60の入出力端子24に接続するための入出力端子601と、各部を制御する制御部605等を備えている。

【0724】

さらに、メモリ製造装置 600 は、メモリ情報記録媒体 60 の ID、秘密鍵、公開鍵証明書、当該媒体 60 の製造時点における最新のリスト及びそのバージョンナンバーを予め格納している鍵・リスト記録媒体 607 とそのドライブ部 606 を備えている。なお、図 92 の構成では、鍵・リスト記録媒体 607 及びドライブ部 606 は、当該メモリ製造装置 600 に内蔵されている例を挙げているが、当該鍵・リスト記録媒体 607 及びドライブ部 606 は外付けの媒体及びドライブであってもよい。上記 ID、秘密鍵、公開鍵証明書、最新のリスト及びバージョンナンバーは、図示しない鍵発行センタにより発行されるものであり、上記内蔵或いは外付けの鍵・リスト記録媒体に予め格納されている。

【0725】

上記鍵・リスト記録媒体 607 に格納されている情報は、制御部 605 の制御の元、ドライブ部 606 により読み取られ、インターフェース部 608 及び入出力端子 601 を介して、メモリ情報記録媒体 60 に送られる。このときのメモリ情報記録媒体 60 では、メモリ製造装置 600 から送られてきた上記 ID、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーを、メモリ部 22 のデータ記録領域に記録する。

【0726】

また、ID、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーは、上述したように内蔵或いは外付けの鍵・リスト記録媒体に予め格納されているものを読み取るだけでなく、例えば鍵発行センタより送られてきたものを外部インターフェース部 609 を介して直接に入手することも可能である。このように、外部インターフェース部 609 を介して ID、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーを入手するようにした場合、当該外部インターフェース部 609 を介した ID、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーは、制御部 605 からインターフェース部 608、入出力端子 601 を介して直接メモリ情報記録媒体 60 に送られ、メモリ部 22 のデータ記録領域に記録されることになる。

【0727】

図93には、本発明の記録媒体製造方法として、上記メディアタイプIM3のメモリ情報記録媒体60を製造すると共に、当該メモリ情報記録媒体60に対して最新のリストを記録するメモリ製造方法における製造工程の流れを示す。

【0728】

図93において、メモリ製造方法では、先ず、ステップS300の製造工程として、図示しない組立工程によりメディアタイプIM3のメモリ情報記録媒体60が組み立てられる。

【0729】

次に、メモリ製造方法では、ステップS301の製造工程として、図92のメモリ製造装置600により、前記ID、秘密鍵、公開鍵証明書、バージョンナンバーを、メディアタイプIM3であるメモリ情報記録媒体60のメモリ部22のデータ記録領域に書き込む。

【0730】

次に、メモリ製造方法では、ステップS302の製造工程として、図92のメモリ製造装置600により、最新のリストをメモリ部22のコンテンツデータ記録用の領域に書き込む。

【0731】

以上により、メモリ情報記録媒体60は、最新版のリストをデータ記録領域に記録した状態で製造工場から出荷されることになる。

【0732】

図94には、メディアタイプIM4のメモリ情報記録媒体20を製造すると共に、当該メモリ情報記録媒体20に対して最新のリストを記録する記録媒体製造装置であるメモリ製造装置610の概略構成を示す。なお、記録する最新のリストは、リボケーションリスト又はレジストレーションリストの一方、或いは、リボケーションリスト及びレジストレーションリストの両方の何れであっても良い。この図94において、図92と同じ構成要素にはそれぞれ同一の指示符号を付している。

【 0 7 3 3 】

この図 9 4 に示すメモリ製造装置 6 1 0 は、図示しない組立工程により既に組み立てられているメモリ情報記録媒体 2 0 に対して、リストを記録する。但し、メディアタイプ IM 4 であるメモリ情報記録媒体 2 0 は、前述したようにセキュリティモジュール 2 3 がリストを格納するための十分な記憶容量を有する不揮発性メモリ (4 4) を備えているため、当該メモリ製造装置 6 1 0 は、メモリ情報記録媒体 2 0 のセキュリティモジュール 2 3 内の不揮発性メモリに上記リストを記録する。

【 0 7 3 4 】

このため、当該メモリ製造装置 6 1 0 は、メモリ情報記録媒体 2 0 に信号を送信するためのインターフェース部 6 1 8 と、メモリ情報記録媒体 2 0 の入出力端子 2 4 に接続するための入出力端子 6 0 1 と、各部を制御する制御部 6 0 5 等を備え、さらに、メモリ情報記録媒体 2 0 の ID、秘密鍵、公開鍵証明書、当該媒体 2 0 の製造時点における最新のリスト及びそのバージョンナンバーを予め格納している鍵・リスト記録媒体 6 0 7 とそのドライブ部 6 0 6 を備えている。なお、この図 9 4 の場合も前記図 9 2 の例と同様に、当該鍵・リスト記録媒体 6 0 7 及びドライブ部 6 0 6 は外付けの媒体及びドライブであってもよい。上記 ID、秘密鍵、公開鍵証明書、最新のリスト及びバージョンナンバーは、図示しない鍵発行センタにより発行されるものであり、上記内蔵或いは外付けの鍵・リスト記録媒体に予め格納されている。

【 0 7 3 5 】

上記鍵・リスト記録媒体 6 0 7 に格納されている情報は、制御部 6 0 5 の制御の元、ドライブ部 6 0 6 により読み取られ、インターフェース部 6 0 8 及び入出力端子 6 0 1 を介して、メモリ情報記録媒体 2 0 に送られる。このときのメモリ情報記録媒体 2 0 では、メモリ製造装置 6 1 0 から送られてきた上記 ID、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーを、セキュリティモジュール 2 3 の不揮発性メモリ (4 4) に記録する。

【 0 7 3 6 】

またこの図 9 4 の例においても前記図 9 2 の例と同様に、ID、秘密鍵、公開

鍵証明書、最新のリスト及びそのバージョンナンバーは、上述した内蔵或いは外付けの鍵・リスト記録媒体に予め格納されているものを読み取るだけでなく、例えば鍵発行センタより送られてきたものを外部インターフェース部 6 0 9 を介して直接に入手することも可能である。このように、外部インターフェース部 6 0 9 を介して I D、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーを入手するようにした場合、当該外部インターフェース部 6 0 9 を介した I D、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーは、制御部 6 0 5 からインターフェース部 6 0 8、入出力端子 6 0 1 を介して直接メモリ情報記録媒体 2 0 に送られ、セキュリティモジュール 2 3 内の不揮発性メモリ (4 4) に記録されることになる。

【 0 7 3 7 】

図 9 5 には、本発明の記録媒体製造方法として、上記メディアタイプ I M 4 のメモリ情報記録媒体 2 0 を製造すると共に、当該メモリ情報記録媒体 2 0 に対して最新のリストを記録するメモリ製造方法における製造工程の流れを示す。

【 0 7 3 8 】

図 9 5 において、メモリ製造方法では、先ず、ステップ S 3 1 0 の製造工程として、図示しない組立工程によりメディアタイプ I M 4 のメモリ情報記録媒体 2 0 が組み立てられる。

【 0 7 3 9 】

次に、メモリ製造方法では、ステップ S 3 1 1 の製造工程として、図 9 4 のメモリ製造装置 6 1 0 により、前記 I D、秘密鍵、公開鍵証明書、バージョンナンバーを、メディアタイプ I M 4 であるメモリ情報記録媒体 2 0 のセキュリティモジュール 2 3 内の不揮発性メモリ 4 4 に書き込む。

【 0 7 4 0 】

次に、メモリ製造方法では、ステップ S 3 1 2 の製造工程として、図 9 4 のメモリ製造装置 6 1 0 により、最新のリストをメモリ情報記録媒体 2 0 のセキュリティモジュール 2 3 内の不揮発性メモリ 4 4 に書き込む。

【 0 7 4 1 】

以上により、メモリ情報記録媒体 2 0 は、最新版のリストをセキュリティモジ

ジュール 23 の不揮発性メモリ 44 に記録した状態で製造工場から出荷されることになる。

【0742】

【発明の効果】

以上に説明したように、本発明によれば、記録媒体にセキュリティモジュールを持たせ、記録媒体上に記録されるデータは個々のデータ毎に異なる暗号鍵で暗号化され、暗号鍵はセキュリティモジュールが安全に保管することができる。

【0743】

また、本発明において、セキュリティモジュールは、データの記録時及び再生時に、記録再生装置と公開鍵暗号技術を用いた相互認証を行い、相手が正当なライセンスを受けた装置であることを確認した上で、暗号鍵を装置に対して与えることにより、不正な装置にはデータを漏らさないようにすることができる。

【0744】

さらに、本発明によれば、信頼できるセンタが発行するリボケーションリスト及び／又はレジストレーションリストを活用することにより、正当な装置だが攻撃されてその装置の秘密が露呈してしまった装置にデータを与えることも防ぐことが可能となる。

【0745】

このため、本発明によれば、映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことが可能である。

【図面の簡単な説明】

【図1】

本発明を適用した実施の形態としてリスト格納用の不揮発性メモリを備えたセキュリティモジュールを有する光ディスク情報記録媒体の構成を示す図である。

【図2】

光ディスク情報記録媒体のセキュリティモジュールであって、リスト格納用の不揮発性メモリを備えたセキュリティモジュールの一例を示すブロック図である。

【図 3】

本発明を適用した実施の形態としてリスト格納用の不揮発性メモリを備えた光ディスク記録再生装置の構成を示すブロック図である。

【図 4】

公開鍵証明書の説明に用いる図である。

【図 5】

リボケーションリストを説明するための図である。

【図 6】

第 1 の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図 7】

第 1 の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図 8】

第 1 の実施の形態の光ディスク情報記録媒体にデータを記録する際の他の例の処理手順の内容を示す図である。

【図 9】

第 1 の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図 1 0】

第 1 の実施の形態の光ディスク情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

【図 1 1】

第 1 の実施の形態の光ディスク情報記録媒体からデータを再生する際の他の例の処理手順の内容を示す図である。

【図 1 2】

本発明を適用した実施の形態としてリスト格納用の不揮発性メモリを備えたセキュリティモジュールを有するメモリ情報記録媒体の構成を示す図である。

【図 13】

メモリ情報記録媒体のセキュリティモジュールであって、リスト格納用の不揮発性メモリを備えたセキュリティモジュールの一例を示すブロック図である。

【図 14】

本発明を適用した実施の形態のメモリ記録再生装置の構成を示すブロック図である。

【図 15】

第 2 の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図 16】

第 2 の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図 17】

第 2 の実施の形態のメモリ情報記録媒体にデータを記録する際の他の例の処理手順の内容を示す図である。

【図 18】

第 2 の実施の形態のメモリ情報記録媒体にデータを記録する際のさらに他の例の処理手順の内容を示す図である。

【図 19】

第 2 の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図 20】

第 2 の実施の形態のメモリ情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

【図 21】

第 2 の実施の形態のメモリ情報記録媒体からデータを再生する際の他の例の処理手順の内容を示す図である。

【図 22】

第 2 の実施の形態のメモリ情報記録媒体からデータを再生する際のさらに他の

例の処理手順の内容を示す図である。

【図 2 3】

レジストレーションリストを説明するための図である。

【図 2 4】

第 3 の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図 2 5】

第 3 の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図 2 6】

第 3 の実施の形態の光ディスク情報記録媒体にデータを記録する際の他の例の処理手順の内容を示す図である。

【図 2 7】

第 3 の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図 2 8】

第 3 の実施の形態の光ディスク情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

【図 2 9】

第 3 の実施の形態の光ディスク情報記録媒体からデータを再生する際の他の例の処理手順の内容を示す図である。

【図 3 0】

第 4 の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図 3 1】

第 4 の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図 3 2】

第 4 の実施の形態のメモリ情報記録媒体にデータを記録する際の他の例の処理

手順の内容を示す図である。

【図 3 3】

第 2 の実施の形態のメモリ情報記録媒体にデータを記録する際のさらに他の例の処理手順の内容を示す図である。

【図 3 4】

第 4 の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図 3 5】

第 4 の実施の形態のメモリ情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

【図 3 6】

第 4 の実施の形態のメモリ情報記録媒体からデータを再生する際の他の例の処理手順の内容を示す図である。

【図 3 7】

第 4 の実施の形態のメモリ情報記録媒体からデータを再生する際のさらに他の例の処理手順の内容を示す図である。

【図 3 8】

リボケーションリスト／レジストレーションリストを説明するための図である。

【図 3 9】

第 5 の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図 4 0】

第 5 の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図 4 1】

第 5 の実施の形態の光ディスク情報記録媒体にデータを記録する際の他の例の処理手順の内容を示す図である。

【図 4 2】

第 5 の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図 4 3】

第 5 の実施の形態の光ディスク情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

【図 4 4】

第 5 の実施の形態の光ディスク情報記録媒体からデータを再生する際の他の例の処理手順の内容を示す図である。

【図 4 5】

第 6 の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図 4 6】

第 6 の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図 4 7】

第 6 の実施の形態のメモリ情報記録媒体にデータを記録する際の他の例の処理手順の内容を示す図である。

【図 4 8】

第 6 の実施の形態のメモリ情報記録媒体にデータを記録する際のさらに他の例の処理手順の内容を示す図である。

【図 4 9】

第 6 の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図 5 0】

第 6 の実施の形態のメモリ情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

【図 5 1】

第 6 の実施の形態のメモリ情報記録媒体からデータを再生する際の他の例の処

理手順の内容を示す図である。

【図 5 2】

第 6 の実施の形態のメモリ情報記録媒体からデータを再生する際のさらに他の例の処理手順の内容を示す図である。

【図 5 3】

リスト格納用の不揮発性メモリを備えないセキュリティモジュールを有する光ディスク情報記録媒体の構成を示す図である。

【図 5 4】

光ディスク情報記録媒体のセキュリティモジュールであって、リスト格納用の不揮発性メモリを備えないセキュリティモジュールの一例を示すブロック図である。

【図 5 5】

リスト格納用の不揮発性メモリを備えないセキュリティモジュールを有するメモリ情報記録媒体の構成を示す図である。

【図 5 6】

メモリ情報記録媒体のセキュリティモジュールであって、リスト格納用の不揮発性メモリを備えないセキュリティモジュールの一例を示すブロック図である。

【図 5 7】

第 7 の実施の形態の光ディスク情報記録媒体とその光ディスク記録再生装置の構成を示すブロック図である。

【図 5 8】

第 7 の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図 5 9】

第 7 の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図 6 0】

第 7 の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図 6 1】

第 8 の実施の形態の光ディスク情報記録媒体とその光ディスク記録再生装置の構成を示すブロック図である。

【図 6 2】

第 8 の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図 6 3】

第 8 の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図 6 4】

第 8 の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図 6 5】

第 9 の実施の形態の光ディスク情報記録媒体とその光ディスク記録再生装置の構成を示すブロック図である。

【図 6 6】

第 9 の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図 6 7】

第 9 の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図 6 8】

第 9 の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図 6 9】

第 1 0 の実施の形態のメモリ情報記録媒体とそのメモリ記録再生装置の構成を示すブロック図である。

【図 7 0】

第 1 0 の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処

理手順の内容を示す図である。

【図 7 1】

第 1 0 の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図 7 2】

第 1 0 の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図 7 3】

第 1 1 の実施の形態のメモリ情報記録媒体とそのメモリ記録再生装置の構成を示すブロック図である。

【図 7 4】

第 1 1 の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図 7 5】

第 1 1 の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図 7 6】

第 1 1 の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図 7 7】

第 1 2 の実施の形態のメモリ情報記録媒体とそのメモリ記録再生装置の構成を示すブロック図である。

【図 7 8】

第 1 2 の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図 7 9】

第 1 2 の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図 80】

第 12 の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図 81】

メディアタイプ IM1 に相当する光ディスク情報記録媒体のセキュリティモジュールにおける処理の流れを示すフローチャートである。

【図 82】

メディアタイプ IM2 に相当する光ディスク情報記録媒体のセキュリティモジュールにおける処理の流れを示すフローチャートである。

【図 83】

メディアタイプ IM3 に相当するメモリ情報記録媒体のセキュリティモジュールにおける処理の流れを示すフローチャートである。

【図 84】

メディアタイプ IM4 に相当するメモリ情報記録媒体のセキュリティモジュールにおける処理の流れを示すフローチャートである。

【図 85】

デバイスタイプ Dev1 及び Dev3 の記録再生装置の処理の流れを示すフローチャートである。

【図 86】

デバイスタイプ Dev2 及び Dev4 の記録再生装置の処理の前半部分の流れを示すフローチャートである。

【図 87】

デバイスタイプ Dev2 及び Dev4 の記録再生装置の処理の後半部分の流れを示すフローチャートである。

【図 88】

メディアタイプ IM1 の光ディスク情報記録媒体に最新のリストを記録する光ディスク製造装置の概略構成を示すブロック図である。

【図 89】

メディアタイプ IM1 の光ディスク情報記録媒体に最新のリストを記録する光

ディスク製造工程の流れを示すフローチャートである。

【図 9 0】

メディアタイプ IM 2 の光ディスク情報記録媒体に最新のリストを記録する光ディスク製造装置の概略構成を示すブロック図である。

【図 9 1】

メディアタイプ IM 2 の光ディスク情報記録媒体に最新のリストを記録する光ディスク製造工程の流れを示すフローチャートである。

【図 9 2】

メディアタイプ IM 3 のメモリ情報記録媒体に最新のリストを記録するメモリ製造装置の概略構成を示すブロック図である。

【図 9 3】

メディアタイプ IM 3 のメモリ情報記録媒体に最新のリストを記録するメモリ製造工程の流れを示すフローチャートである。

【図 9 4】

メディアタイプ IM 4 のメモリ情報記録媒体に最新のリストを記録するメモリ製造装置の概略構成を示すブロック図である。

【図 9 5】

メディアタイプ IM 4 のメモリ情報記録媒体に最新のリストを記録するメモリ製造工程の流れを示すフローチャートである。

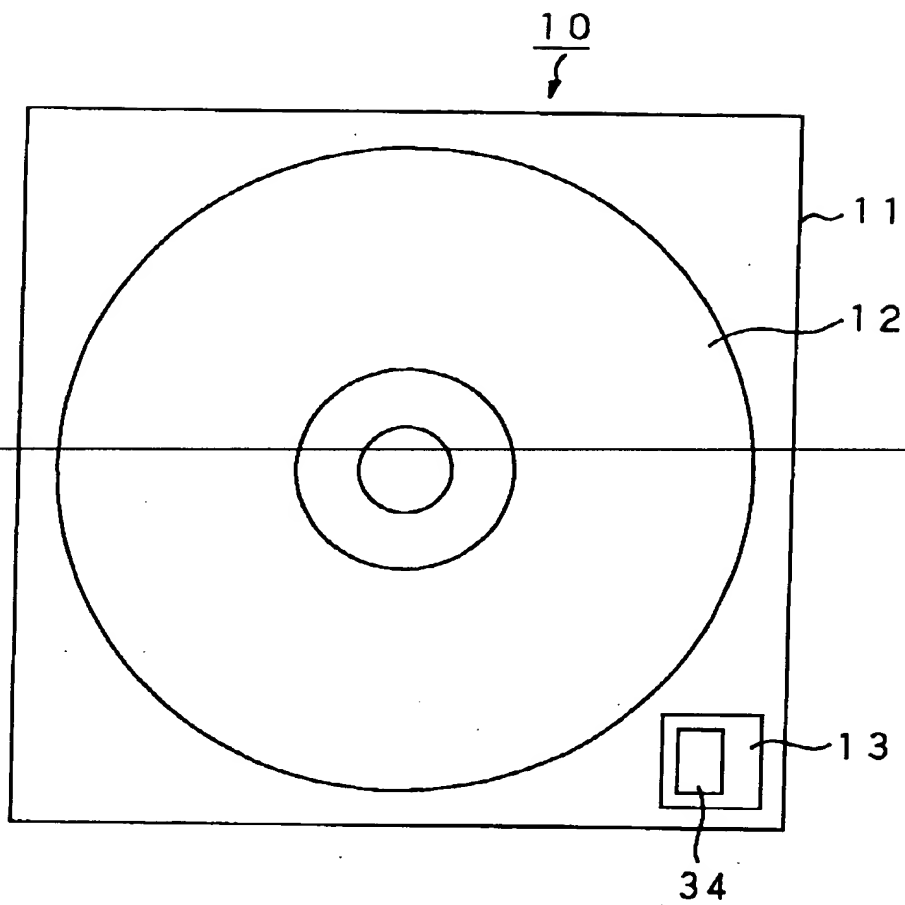
【符号の説明】

1 0, 5 0 光ディスク情報記録媒体、1 1 カートリッジ、1 2 光ディスク、1 3, 2 3, 5 3, 6 3 セキュリティモジュール、3 1 インターフェース部、3 2 演算部、3 3 乱数発生部、3 4 不揮発性メモリ、3 5 制御部、3 4, 4 4, 1 1 0, 2 1 0 不揮発性メモリ、1 0 0, 3 0 0 光ディスク記録再生装置、1 0 1 スピンドルモータ、1 0 2 光学ヘッド、1 0 3 サーボ回路、1 0 4 記録／再生回路、1 0 5 制御部、1 0 6 入力部、1 0 7 乱数発生部、1 0 8 インターフェース部、1 0 9 演算部 1 0 9、2 0, 6 0 メモリ情報記録媒体、2 1 カートリッジ、2 4 入出力端子、4 1 外部インターフェース部、4 2 演算部、4 3 乱数発生部、4 5 制御部、4 6 記

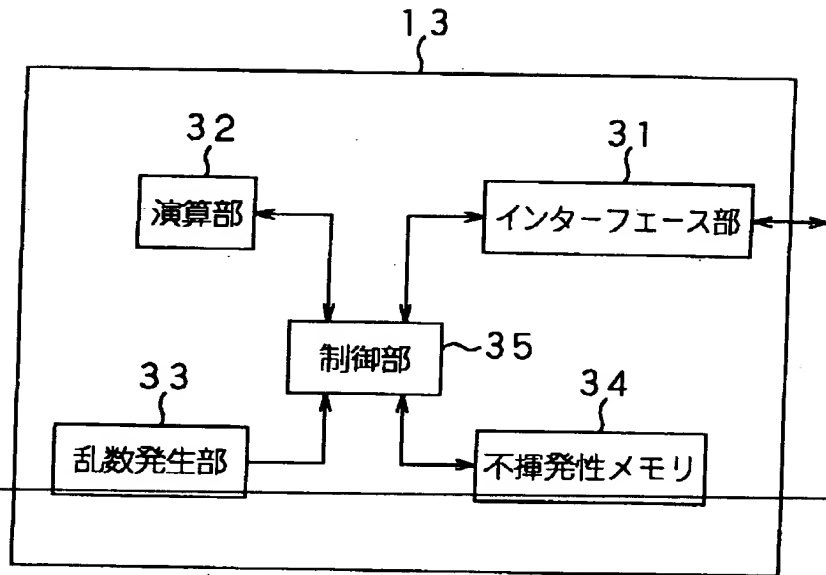
録媒体インターフェース部、200, 400 メモリ記録再生装置、201 入
出力端子、205 制御部、206 入力部、207 乱数発生部、208 イ
ンターフェース部、209 演算部、500, 510 光ディスク製造装置、
600, 610 メモリ製造装置

【書類名】 図面

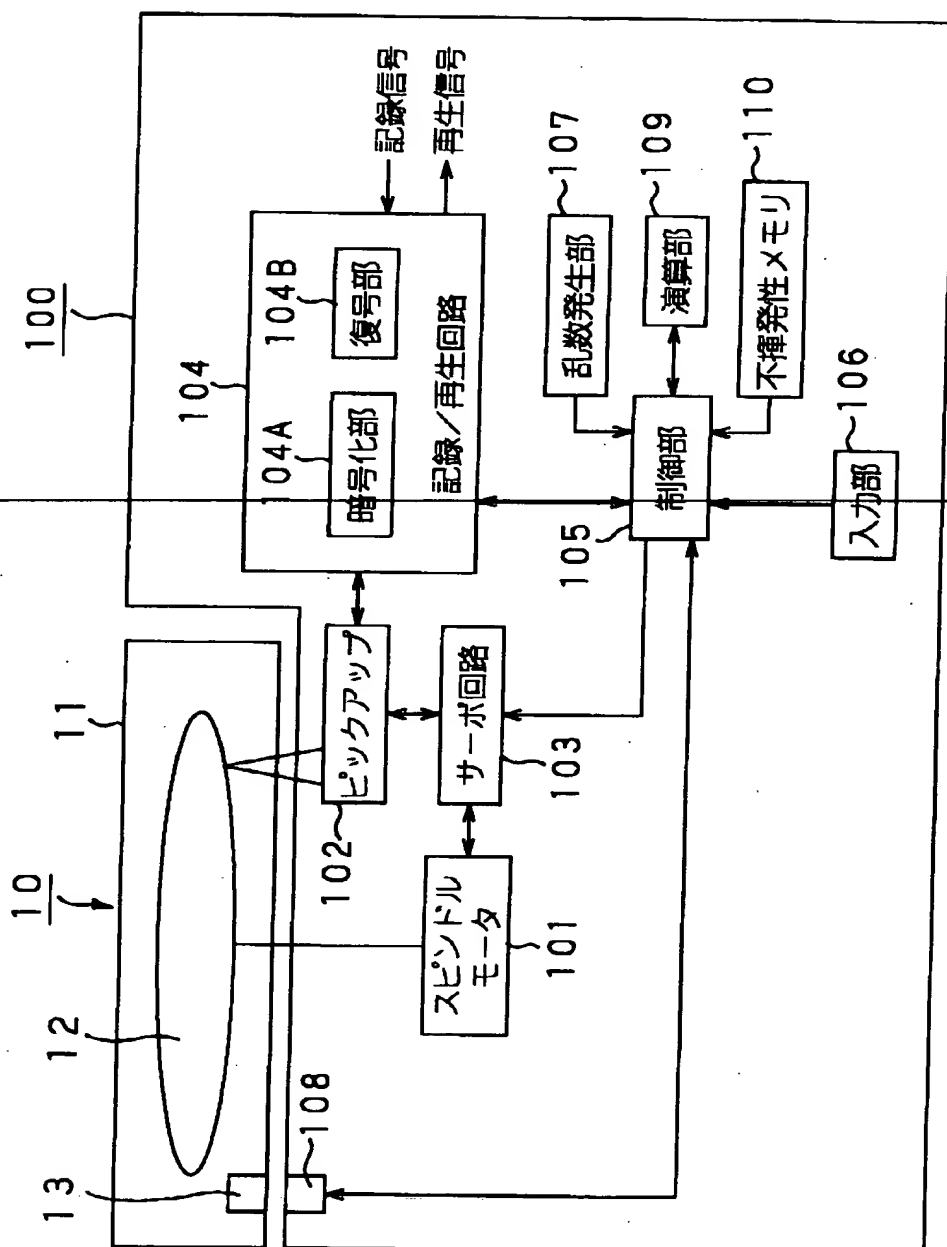
【図 1】



【図 2】



【図 3】



【図 4】

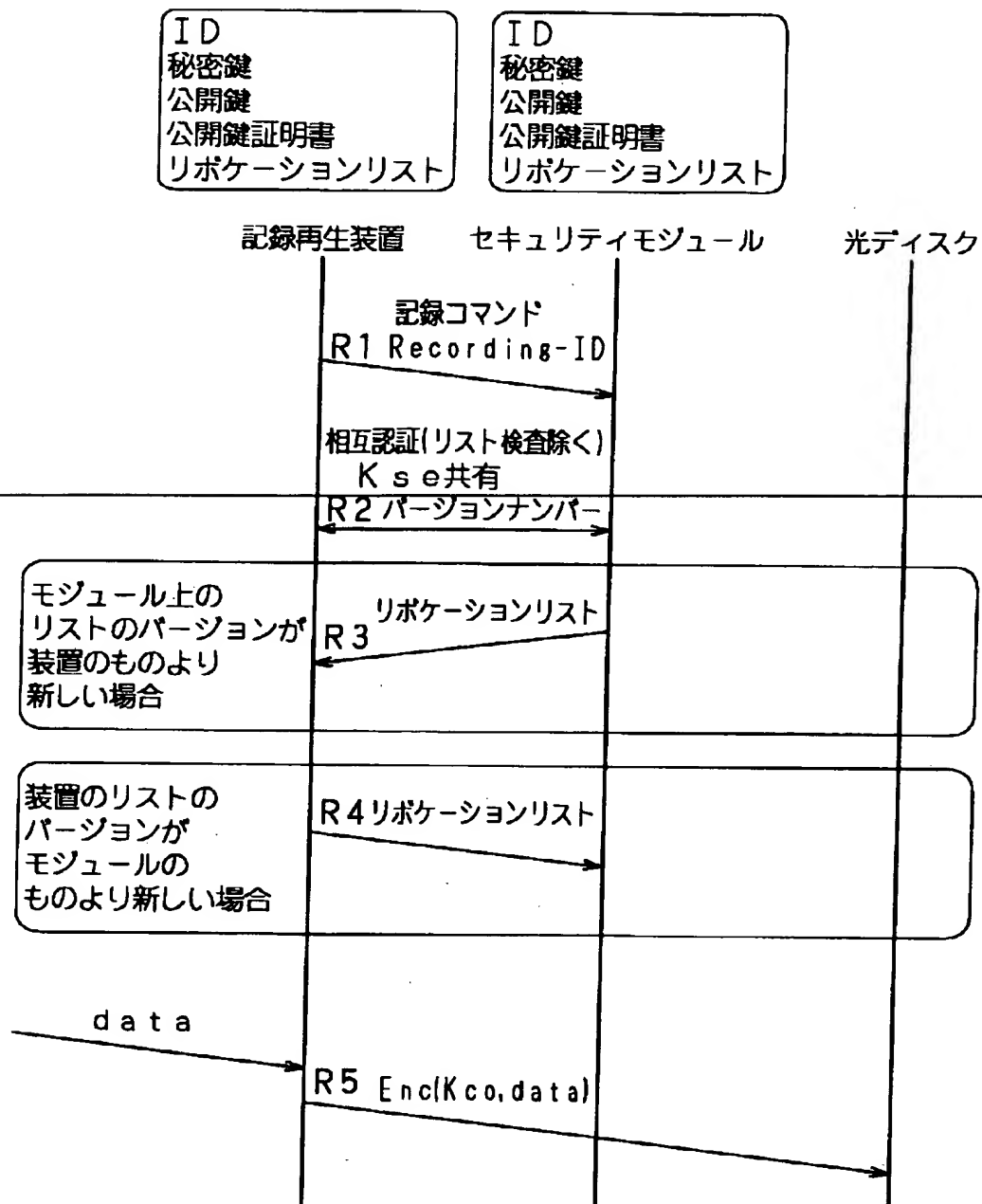
エンティティID
エンティティタイプ
エンティティ公開鍵
TCのデジタル署名

【図 5】

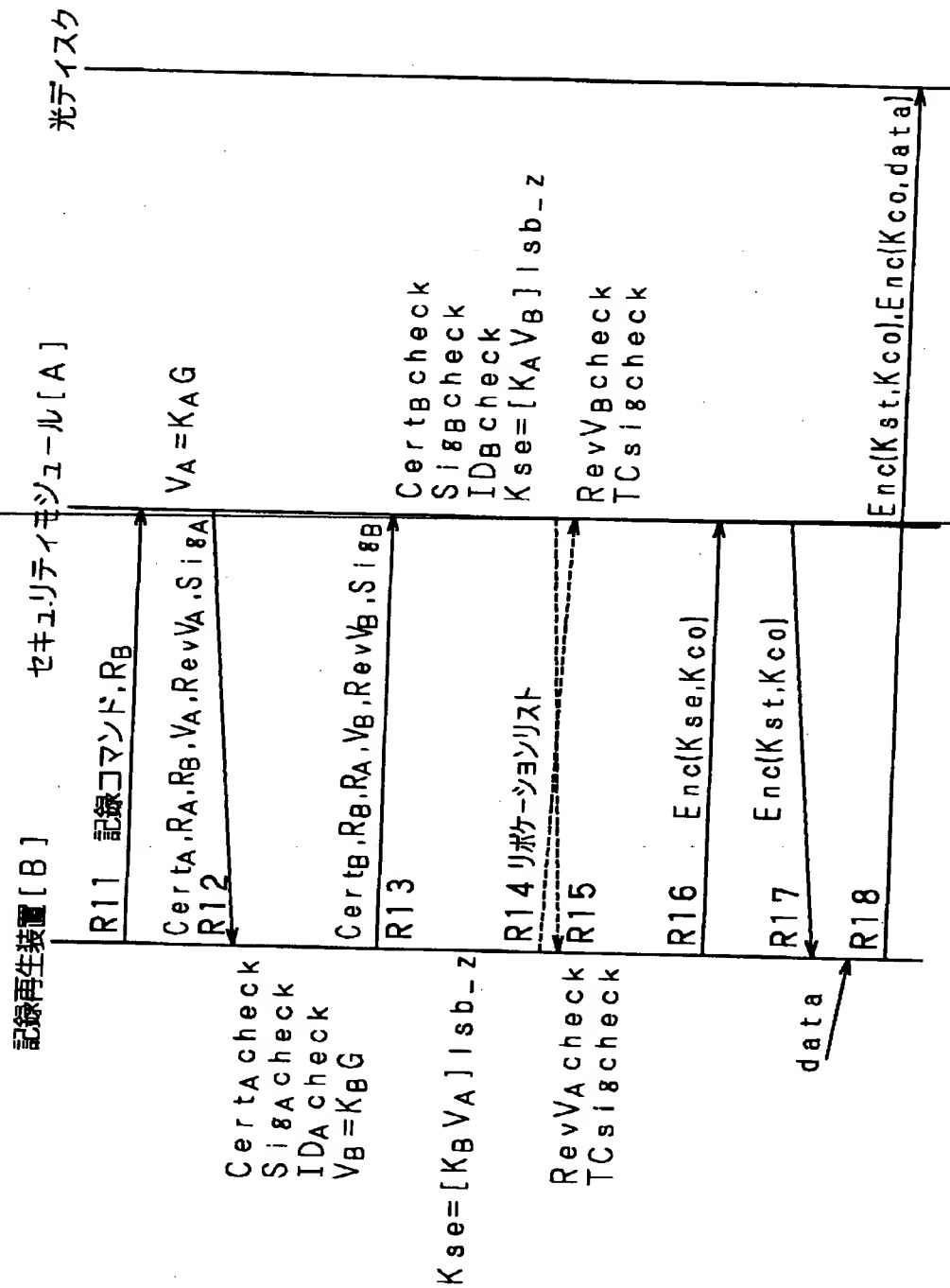
リボケーションリスト

バージョンナンバー
リボークされる機器または媒体のID
.....
TCのデジタル署名

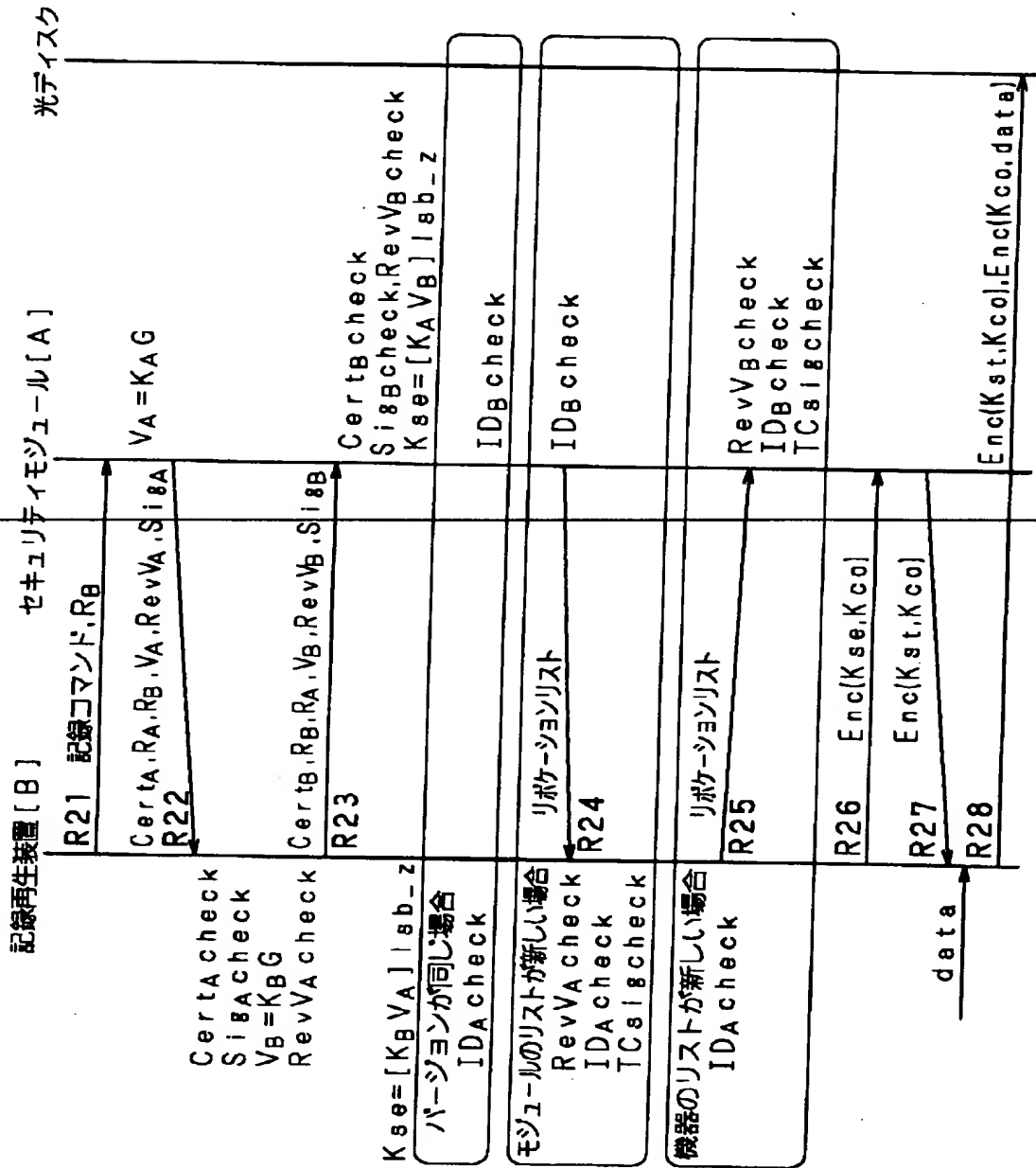
【図 6】



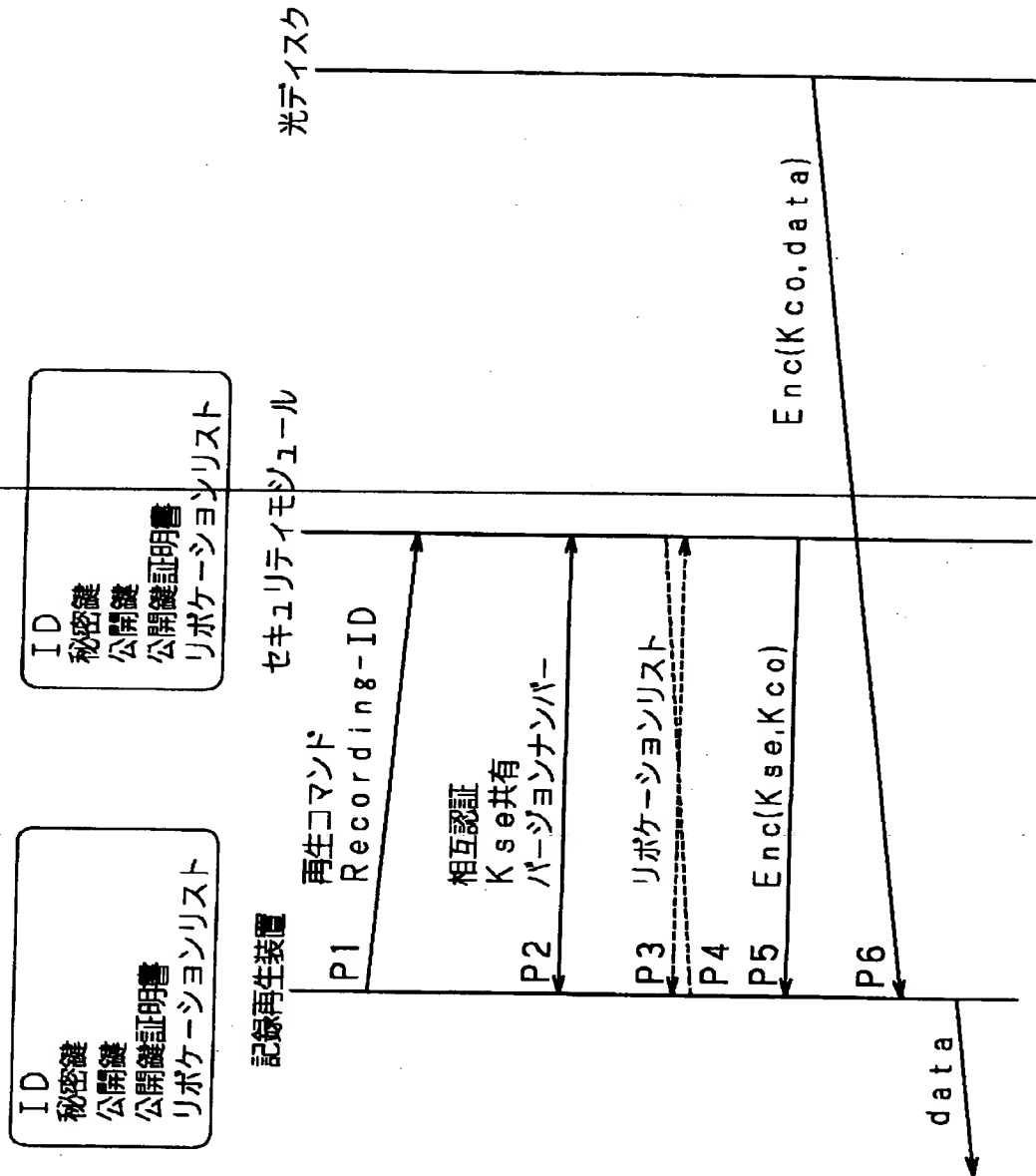
【図 7】



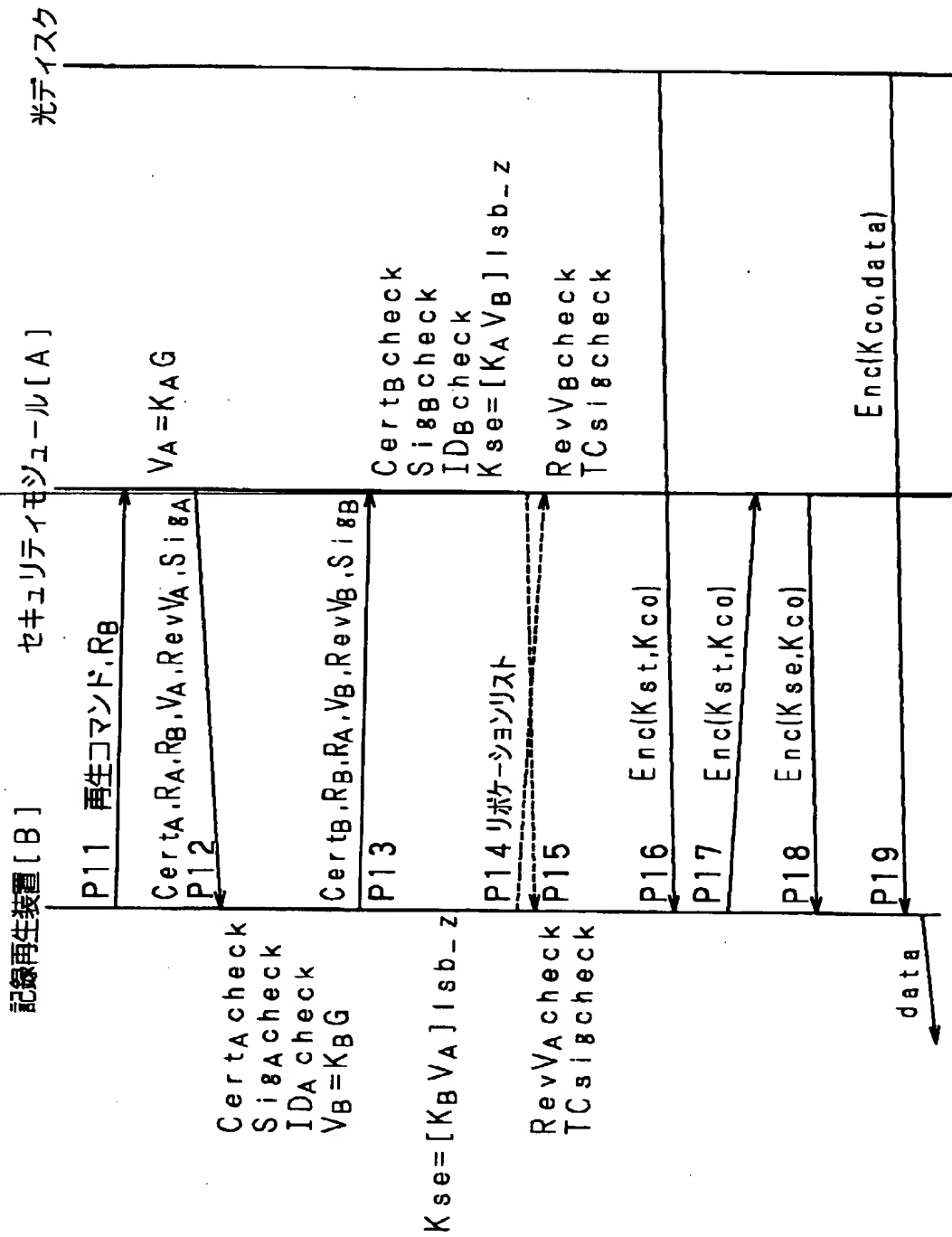
【図 8】



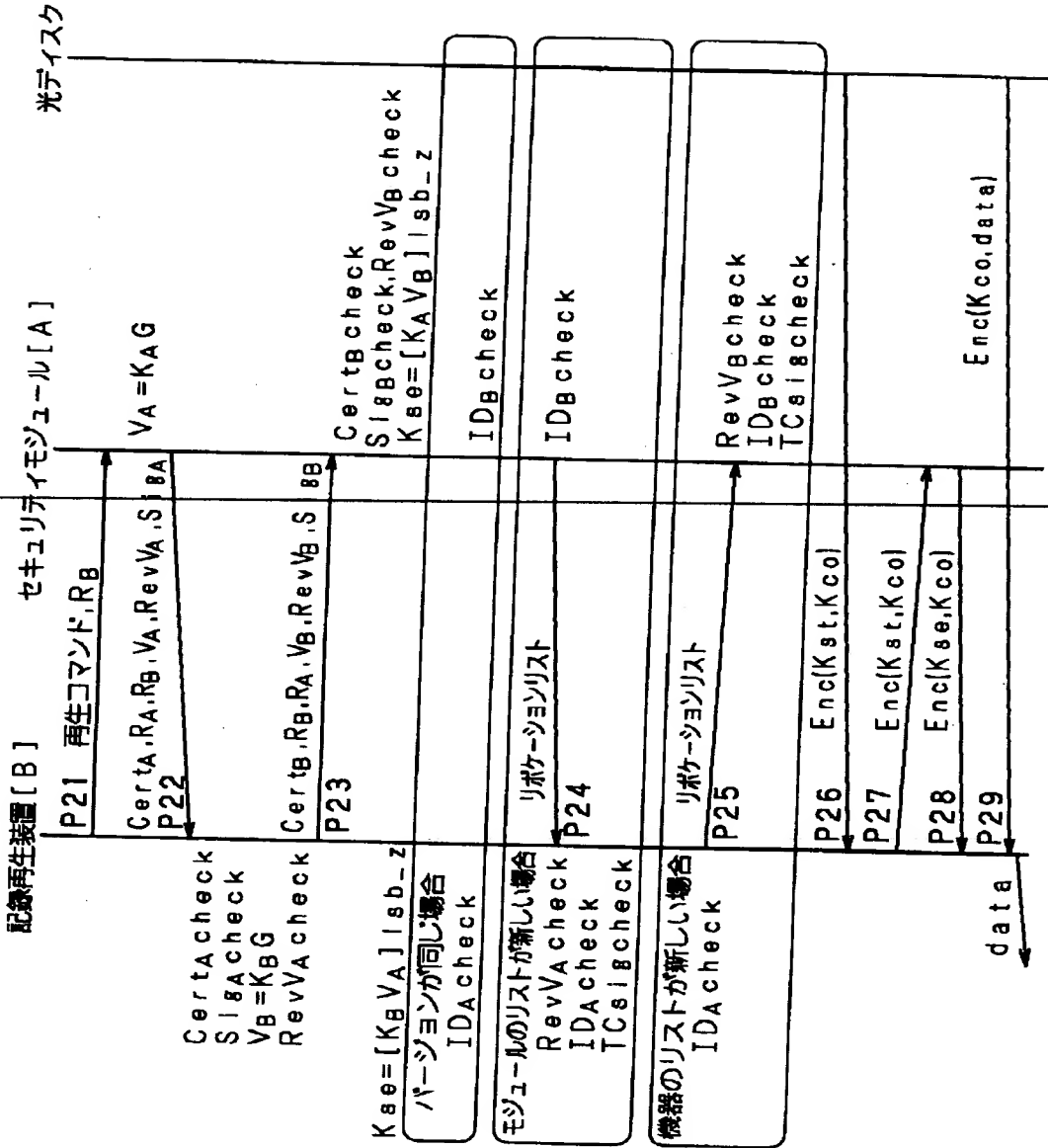
【図 9】



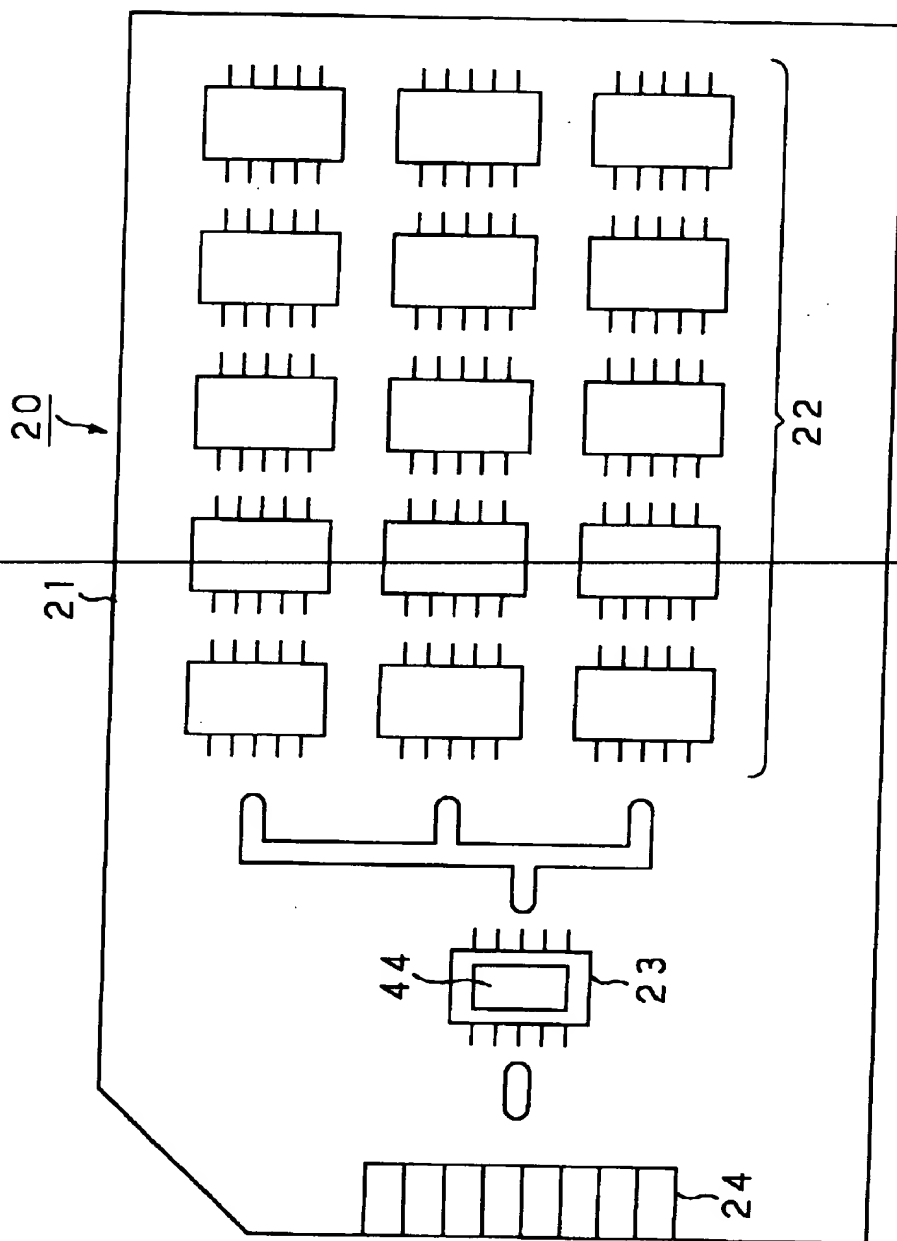
【図 10】



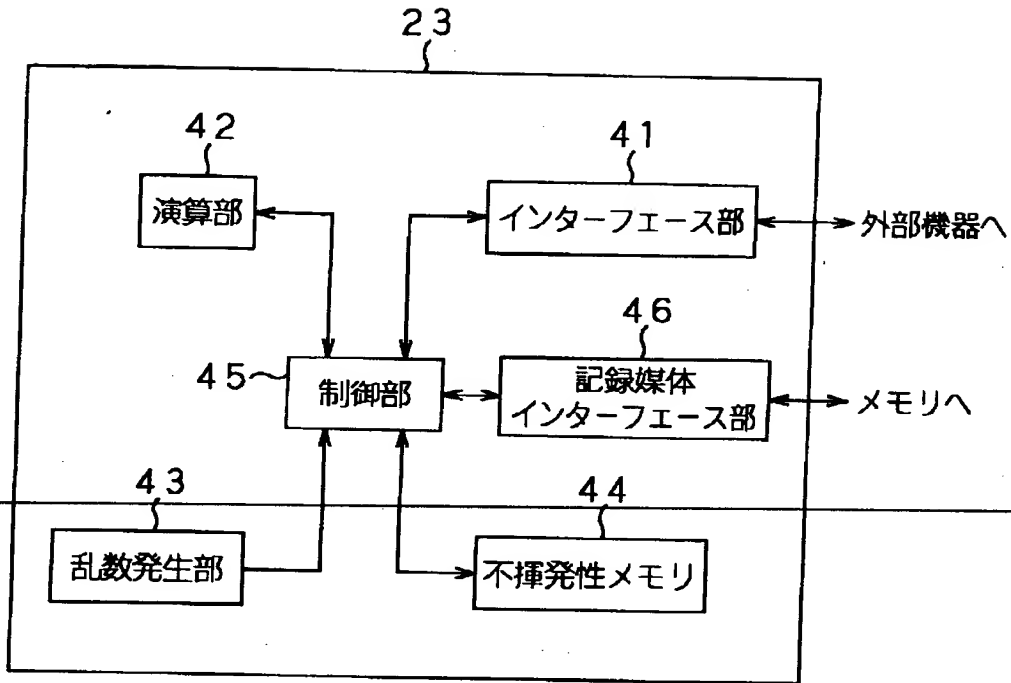
【図 1 1】



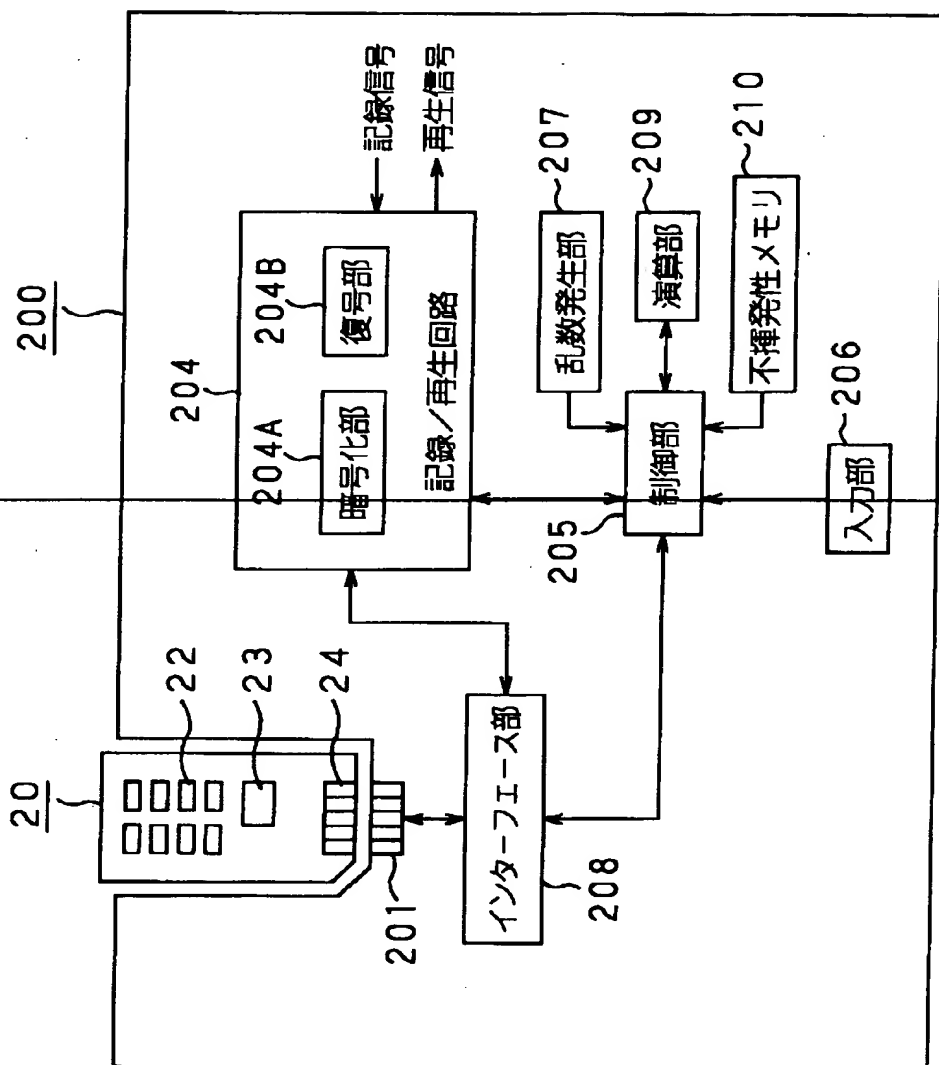
【図 1 2】



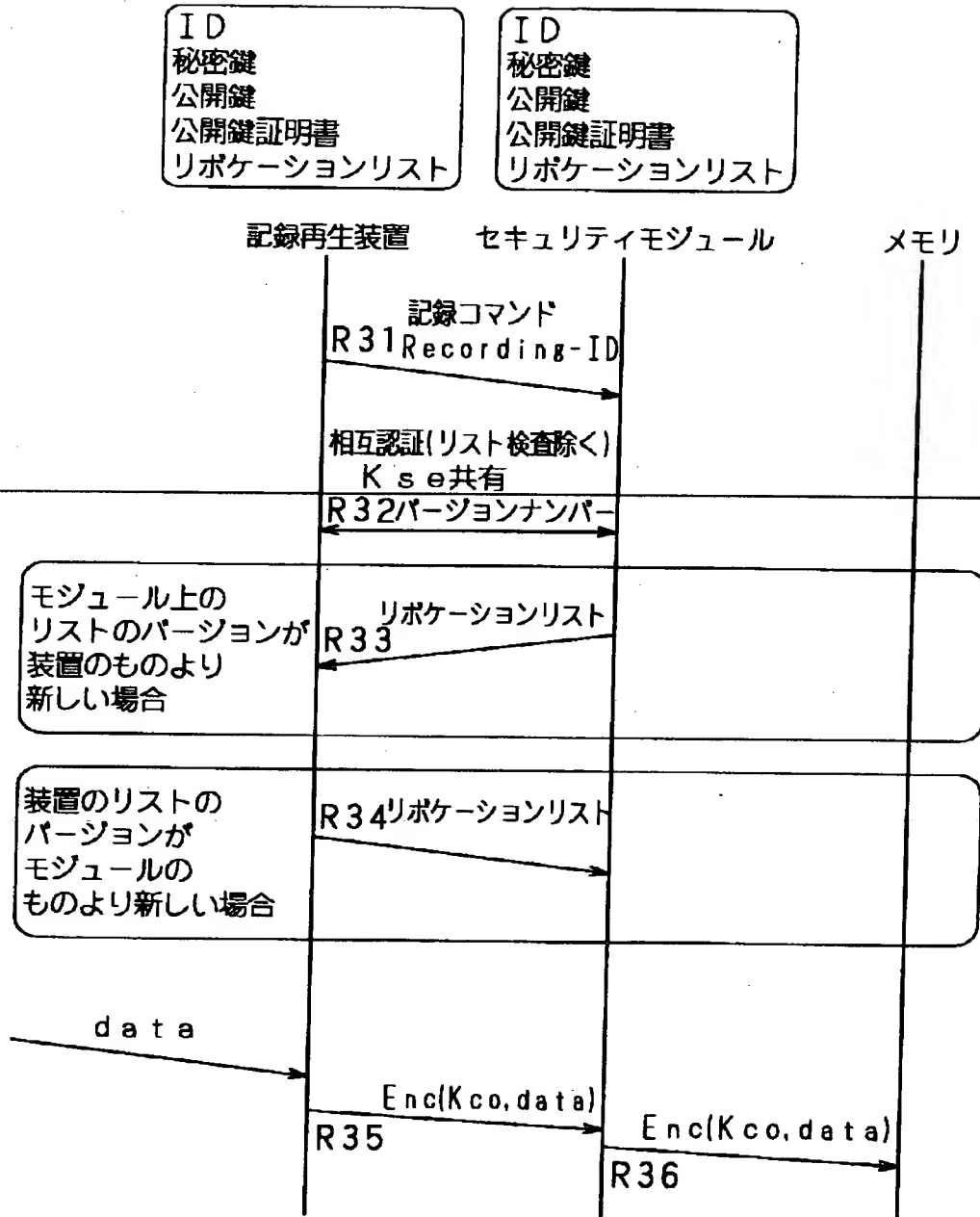
【図 1 3】



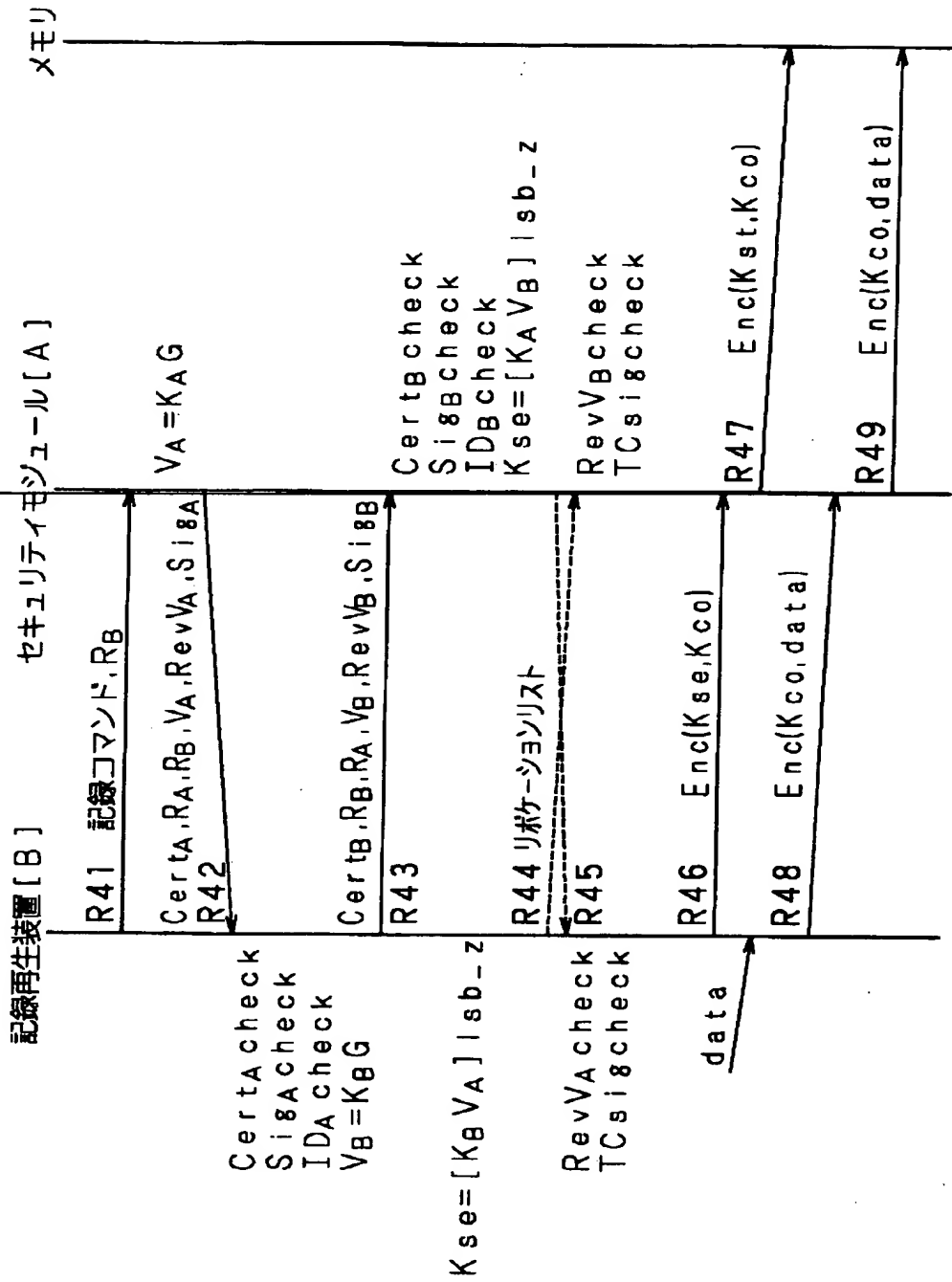
【図 1 4】



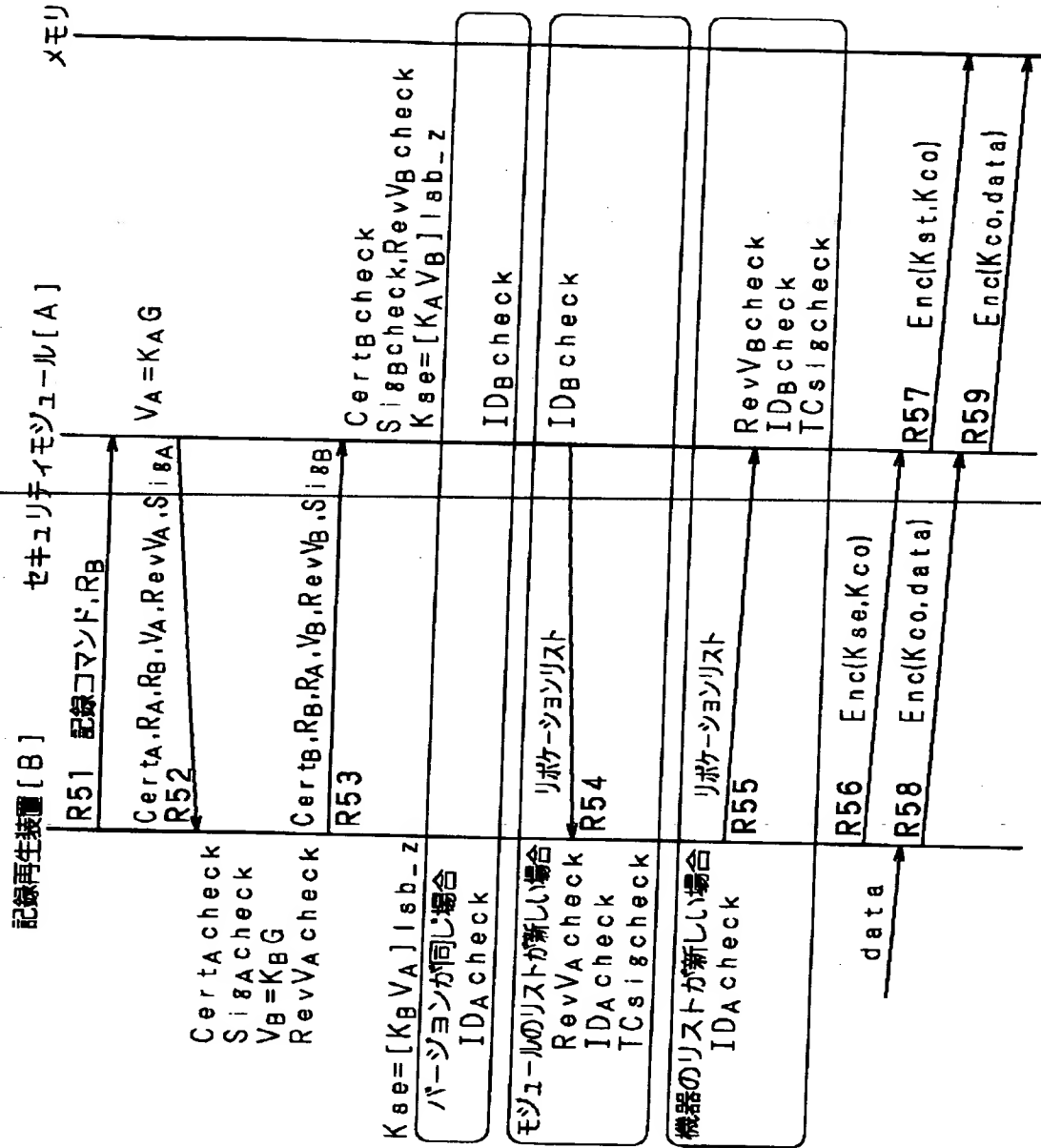
【図 1 5】



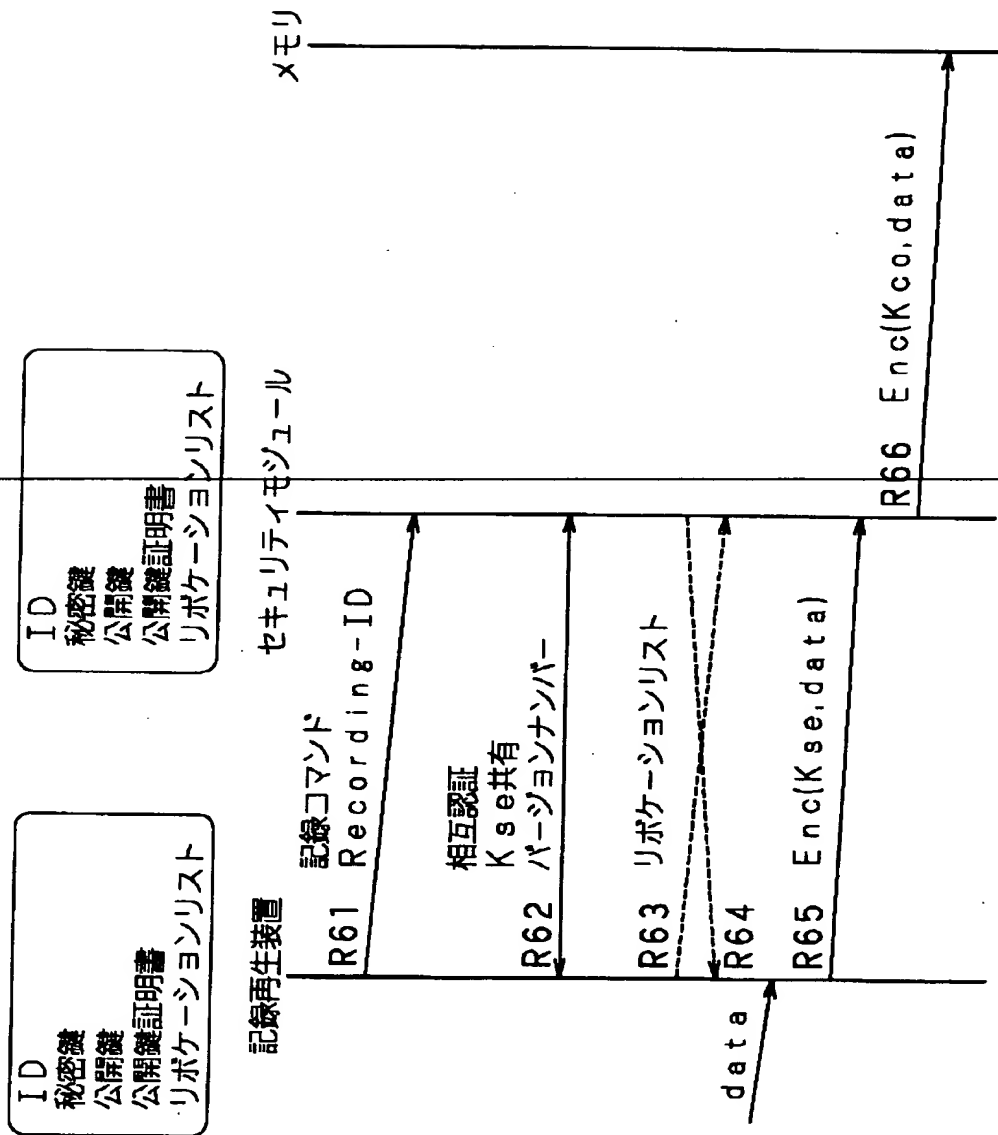
【図 1 6】



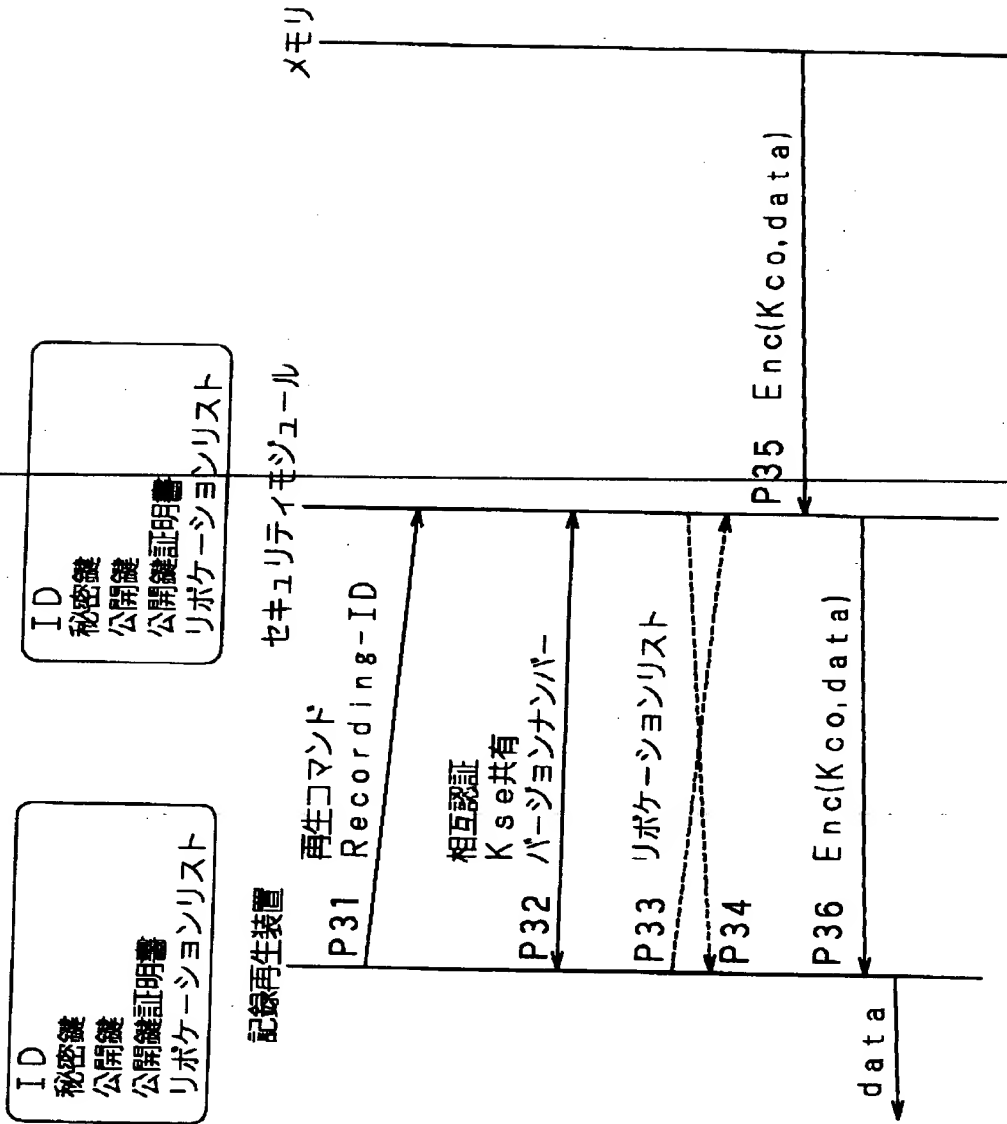
【図 1 7】



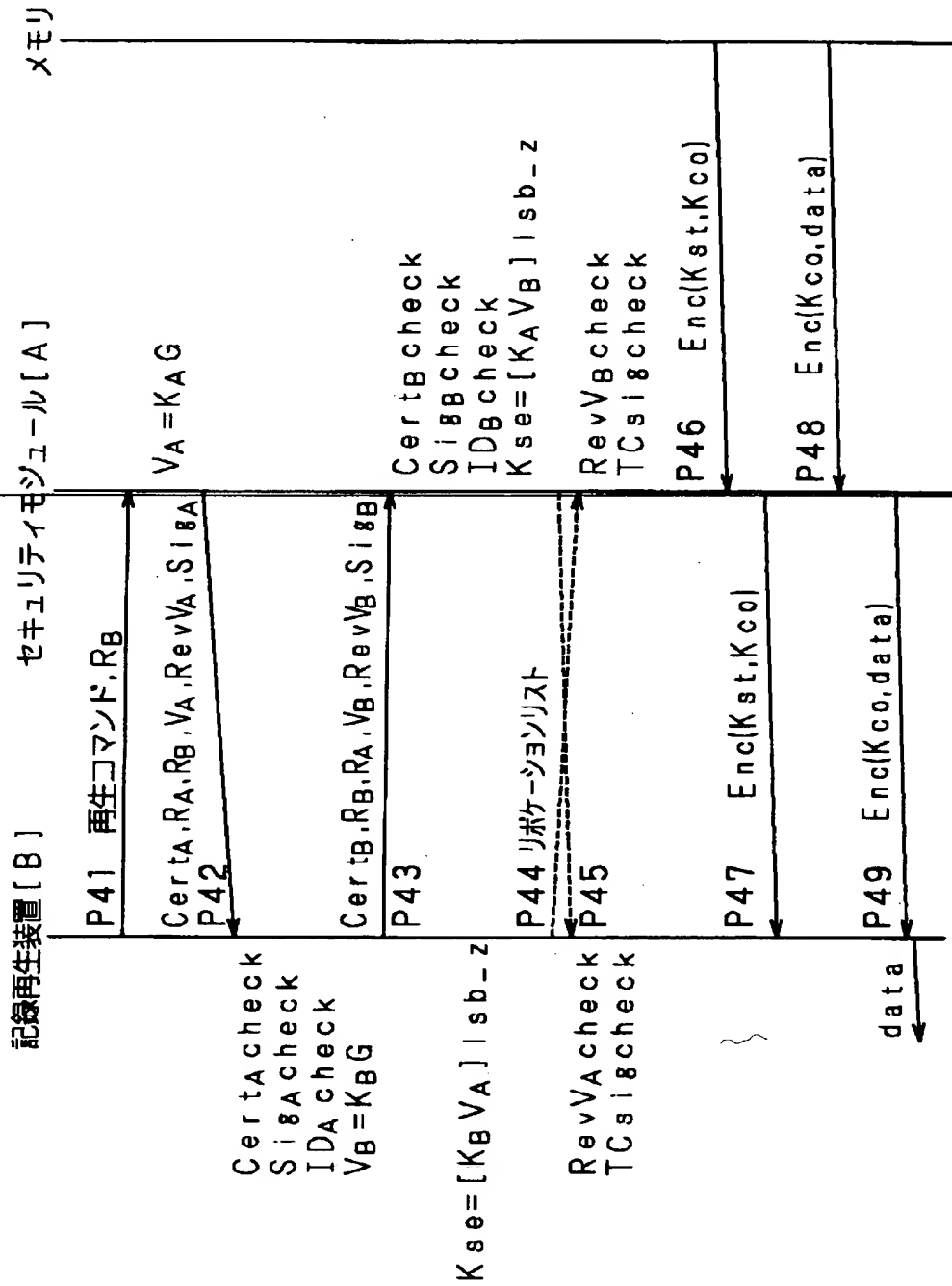
【図 1 8】



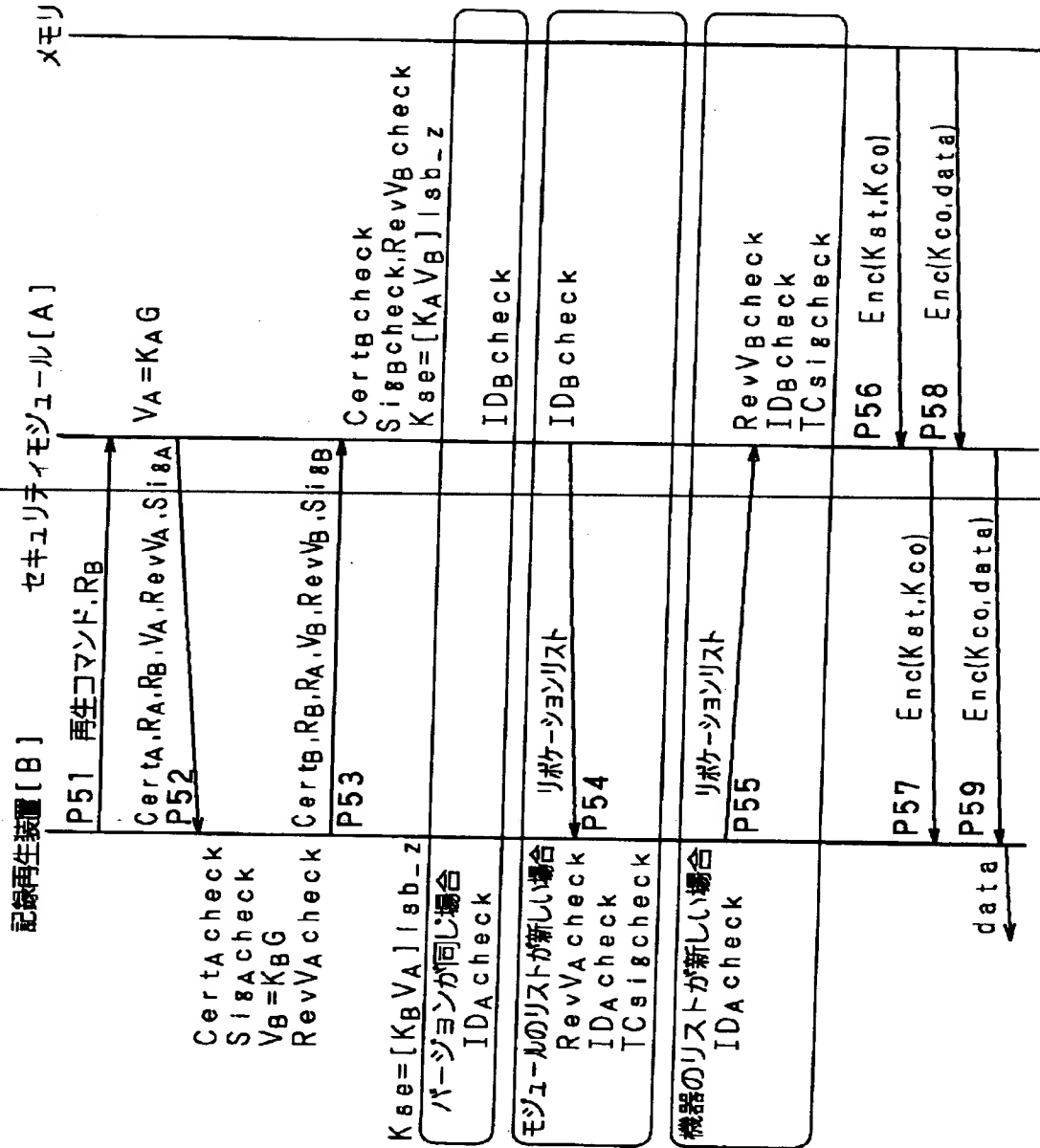
【図 19】



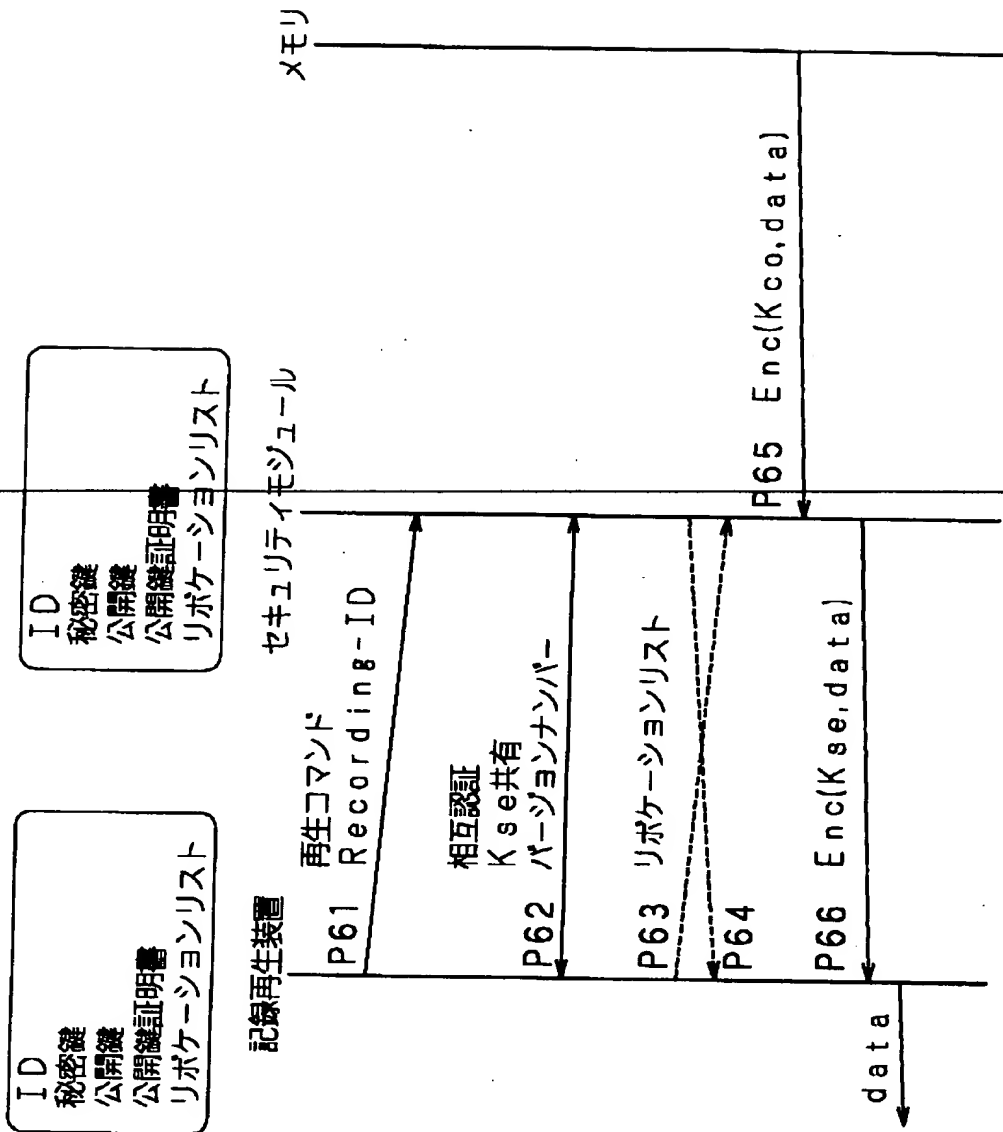
【図 20】



【図 2 1】



【図 2 2】

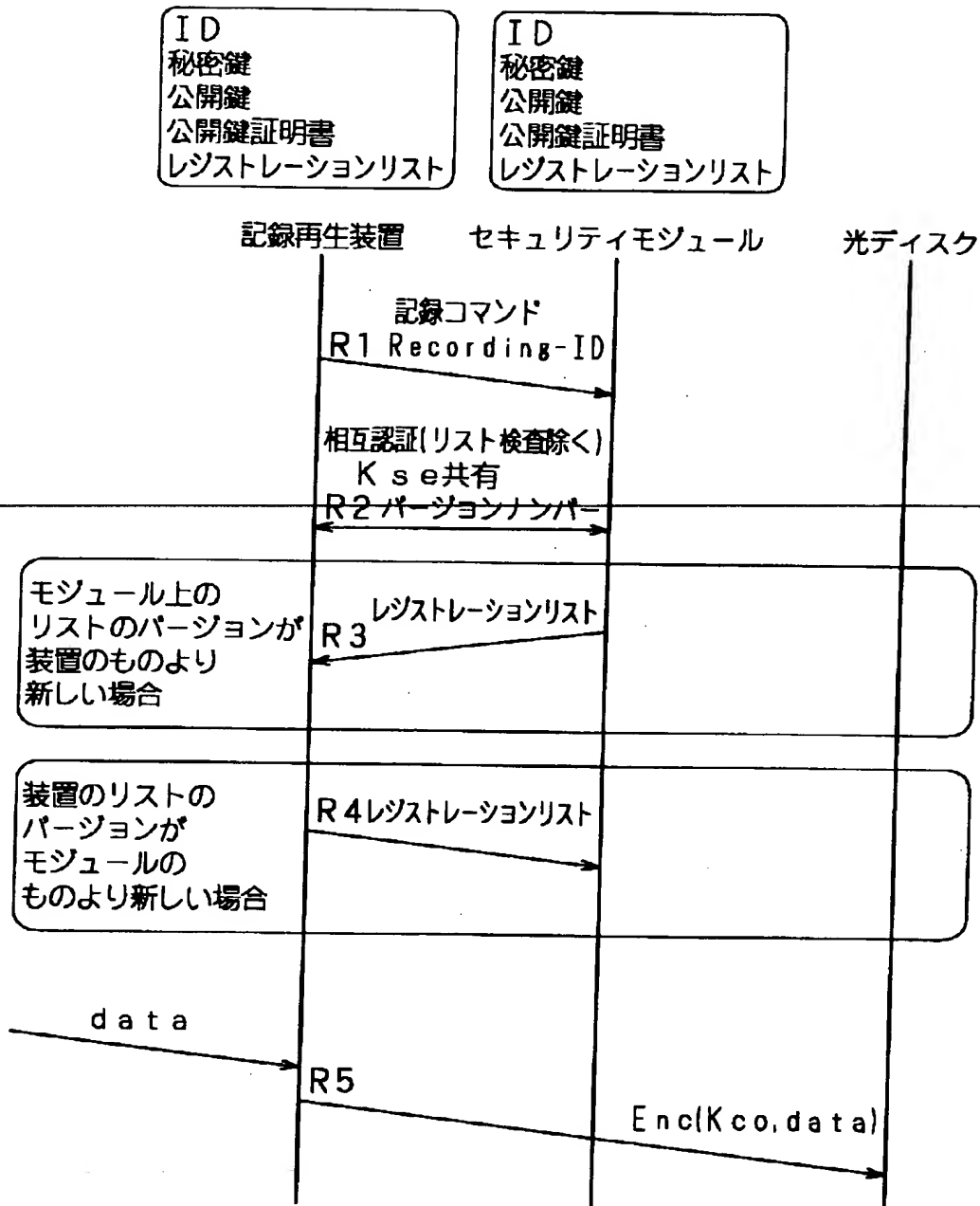


【図 2 3】

レジストレーションリスト

バージョンナンバー
登録される機器または媒体の I D
.
T C のデジタル署名

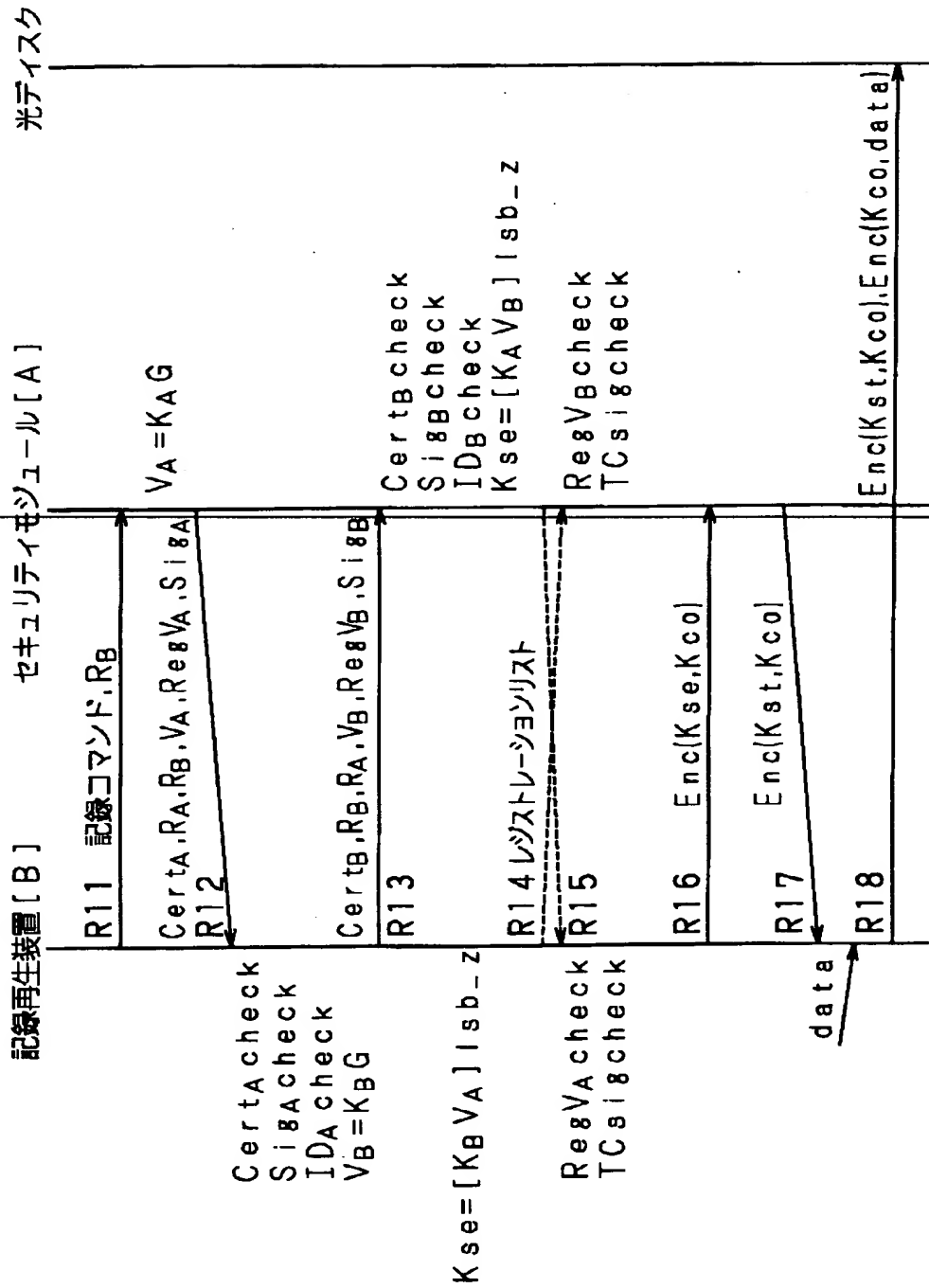
【図 2 4】



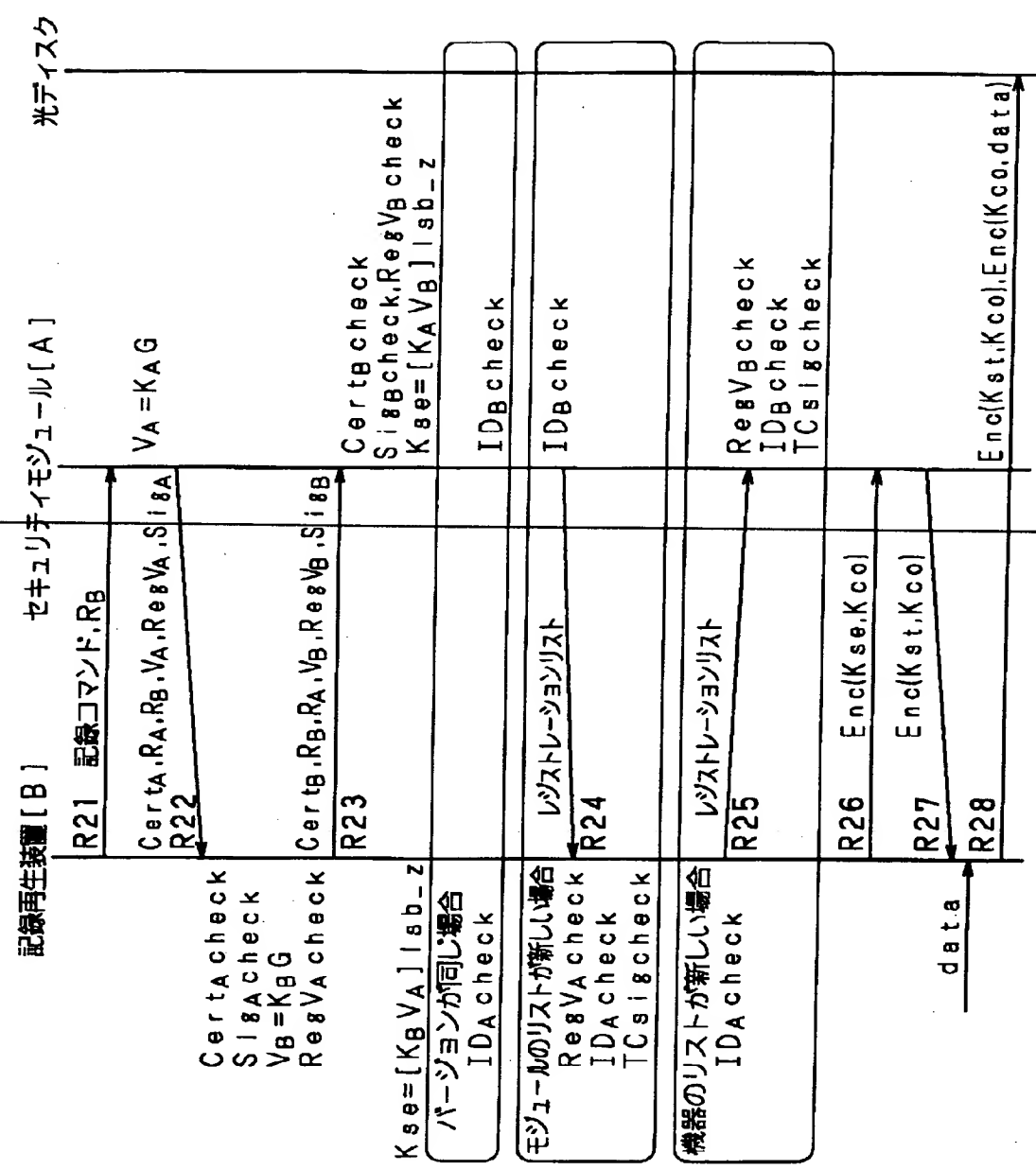


...

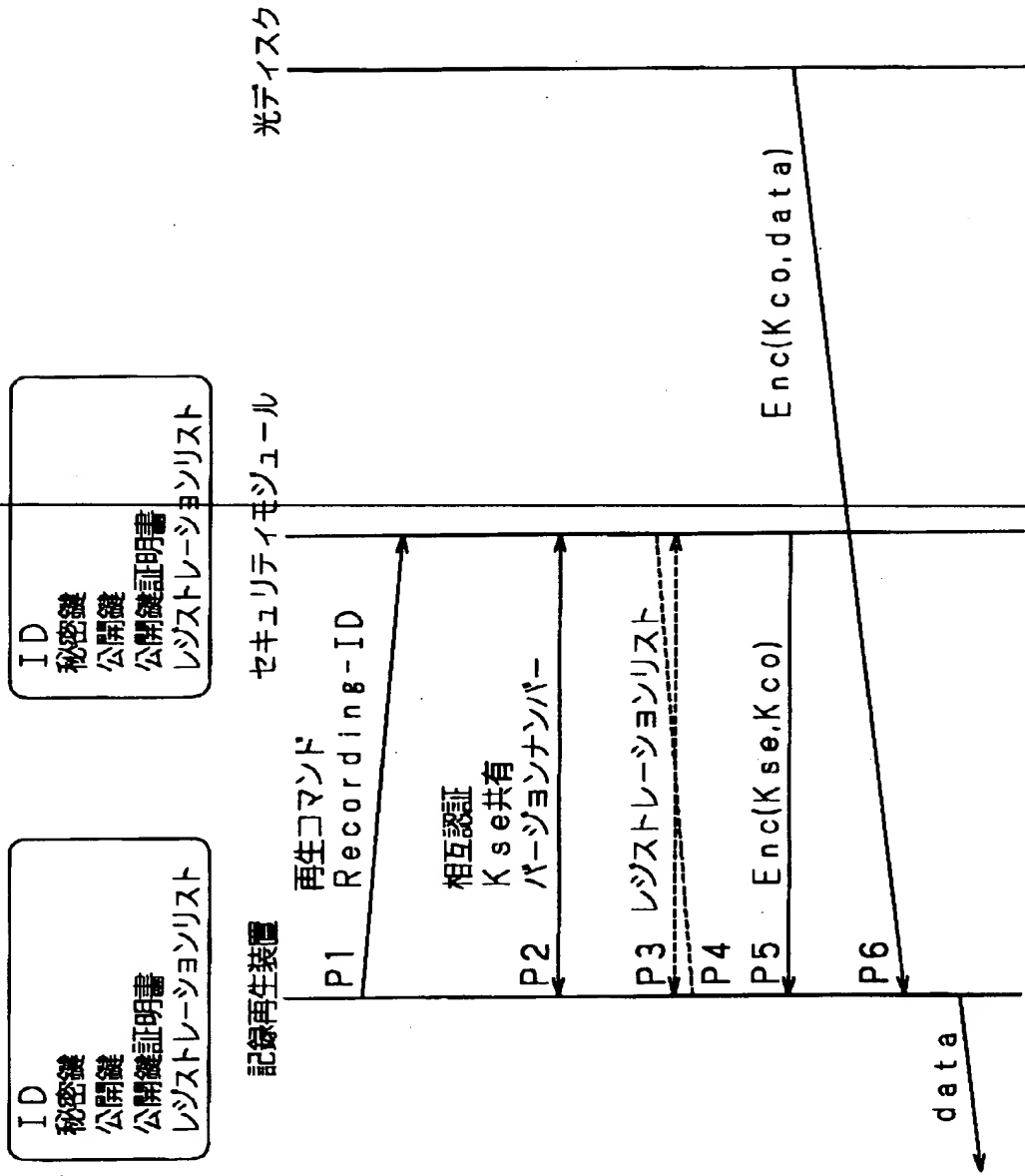
【図 2 5】



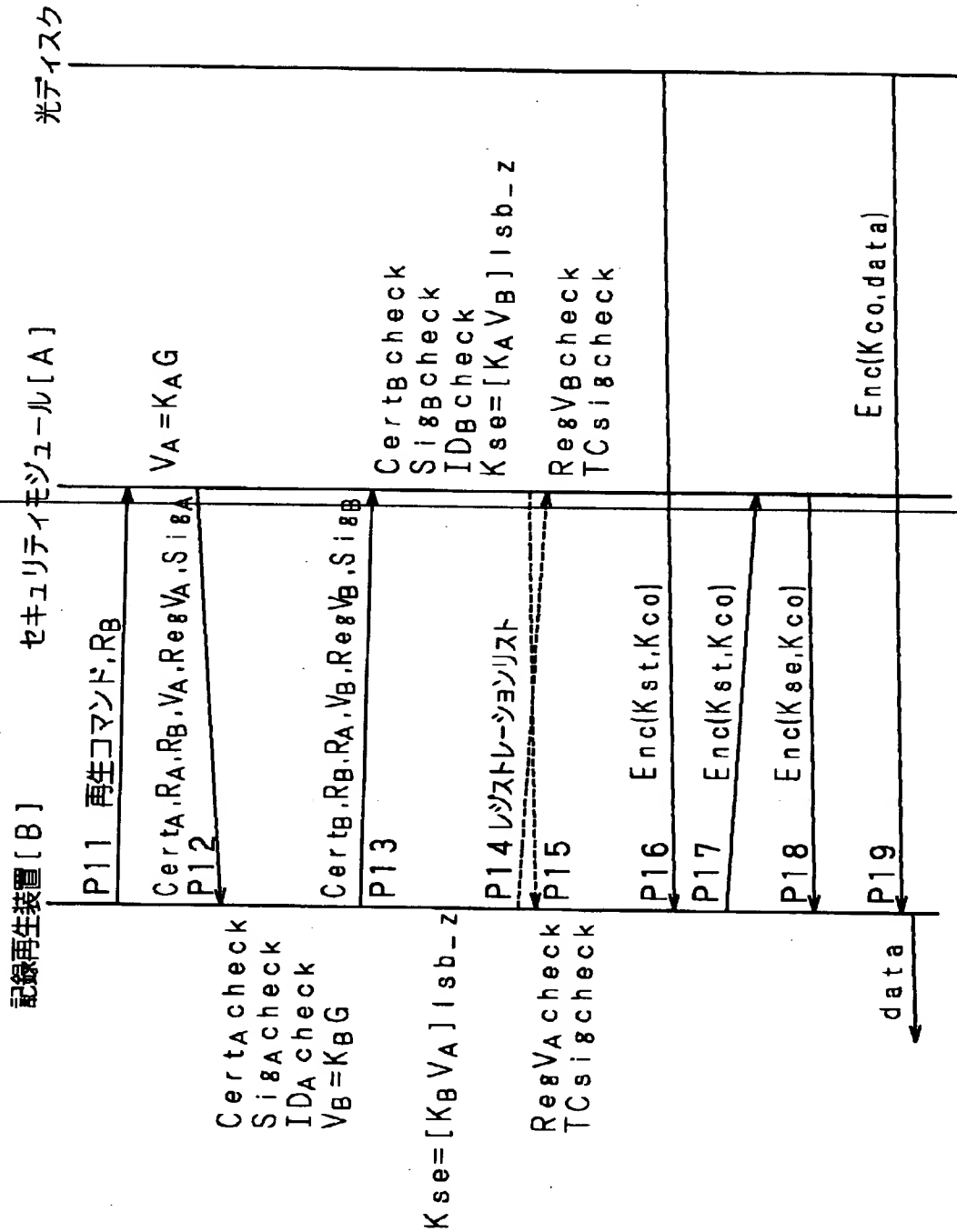
【図 2 6】



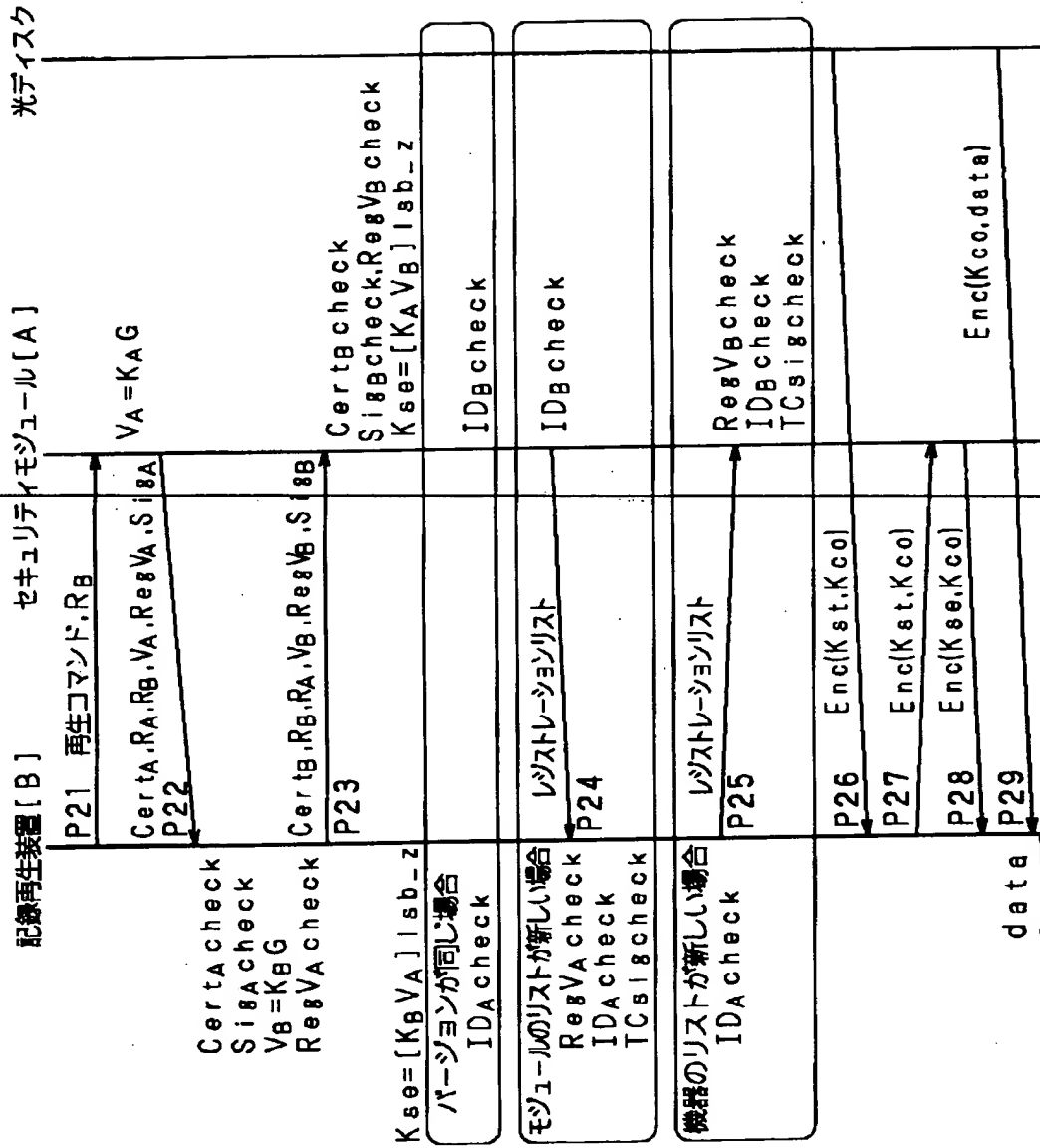
【図 2 7】



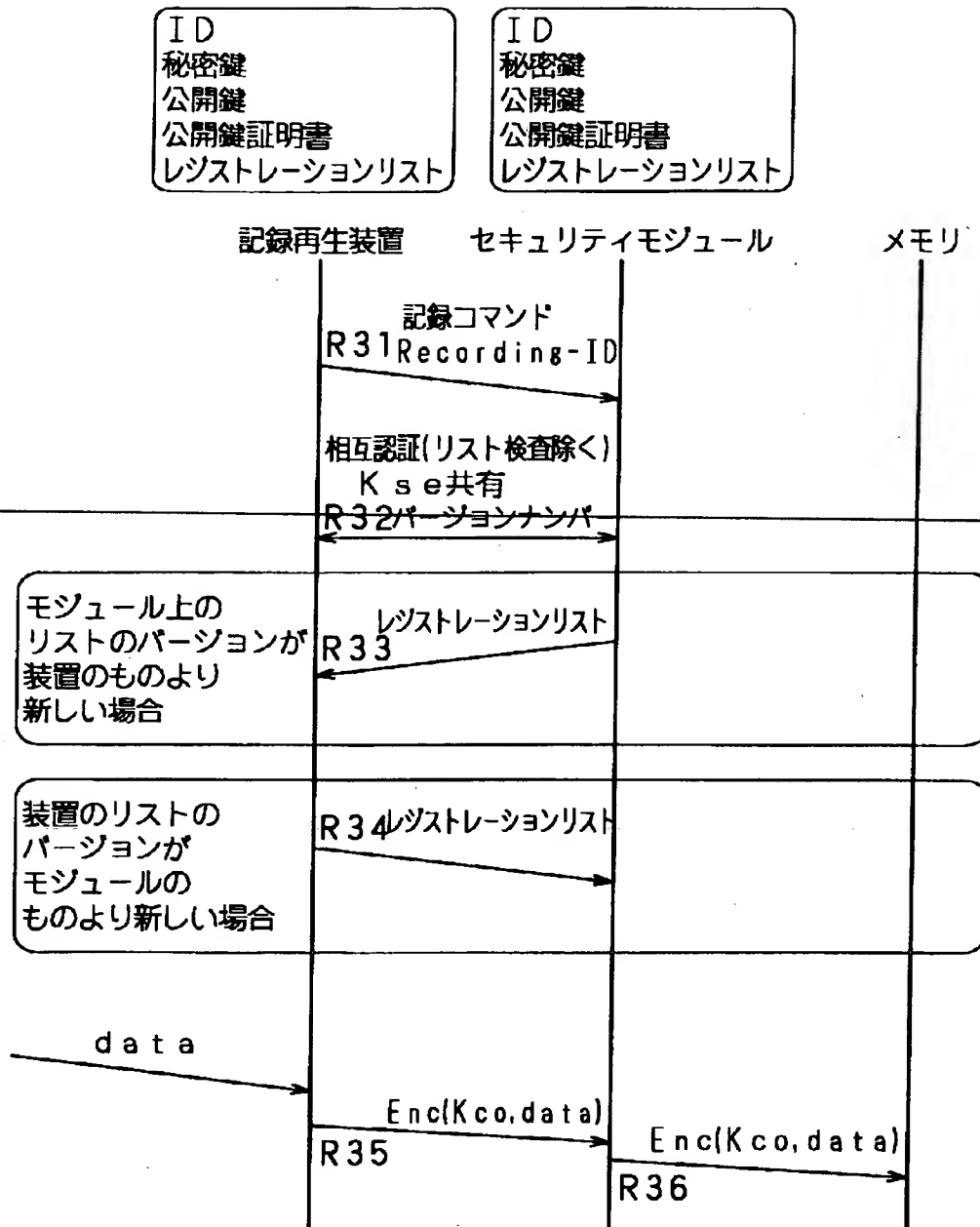
【図 2 8】



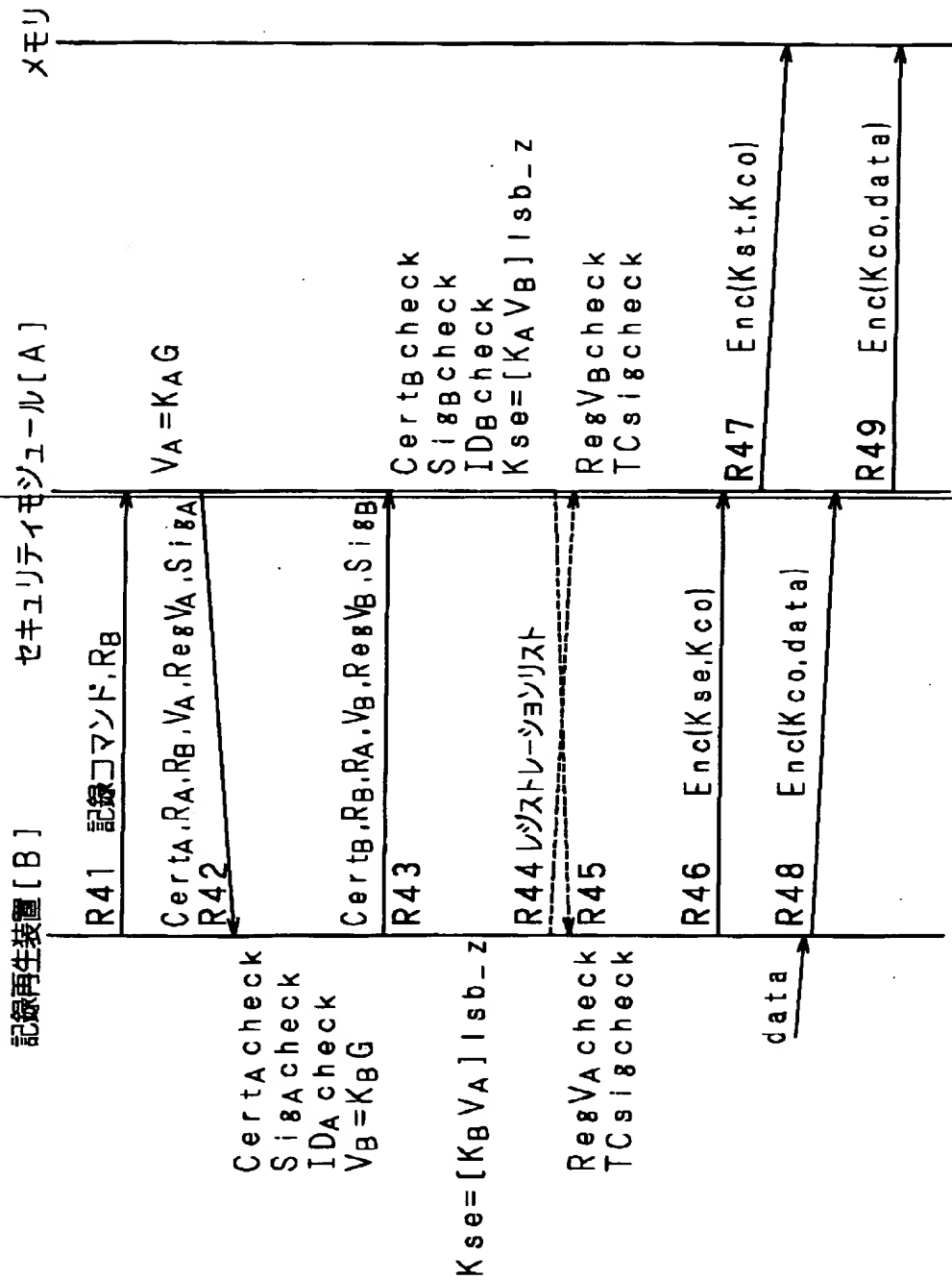
【図 2 9】



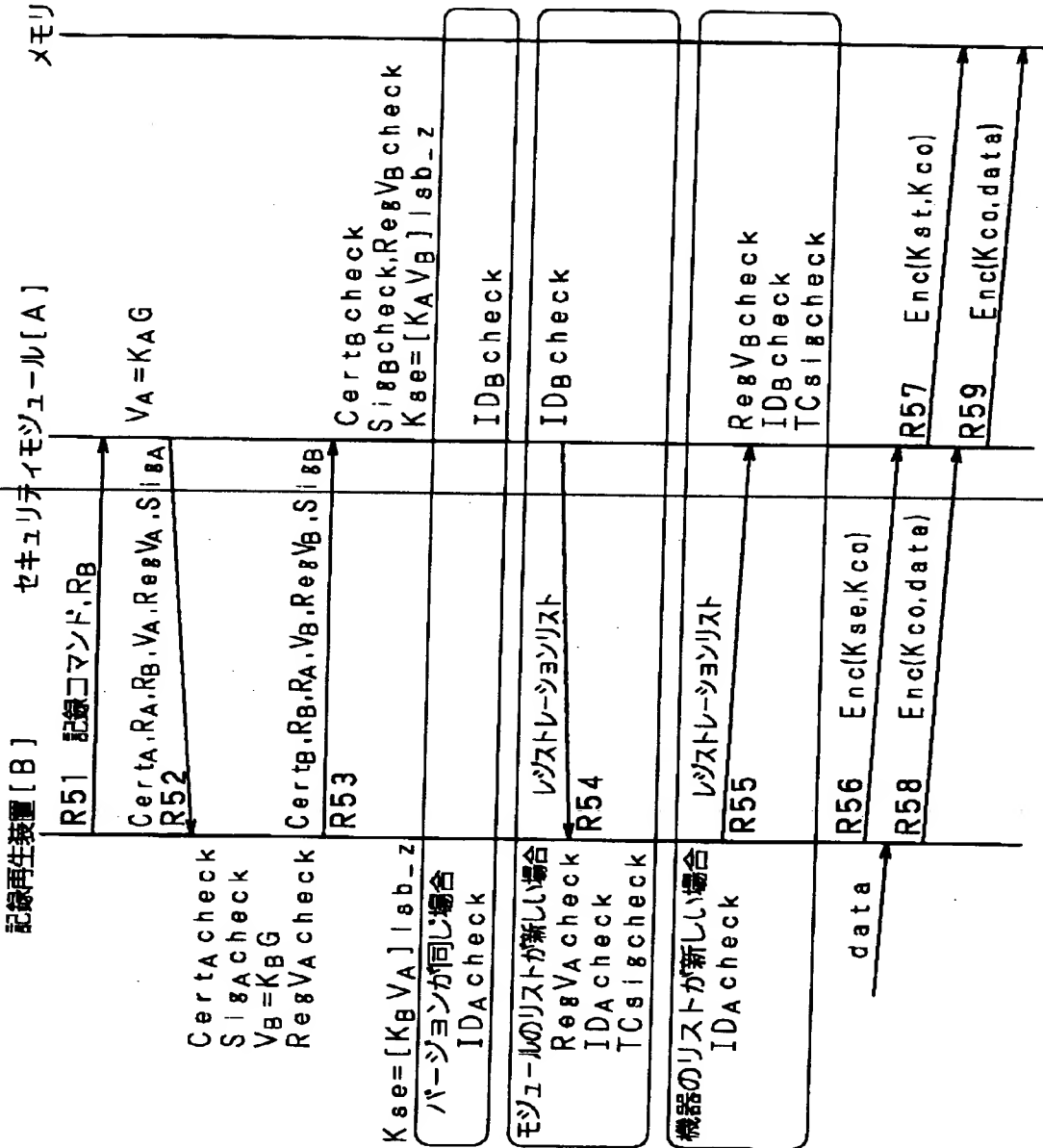
【図 3 0】



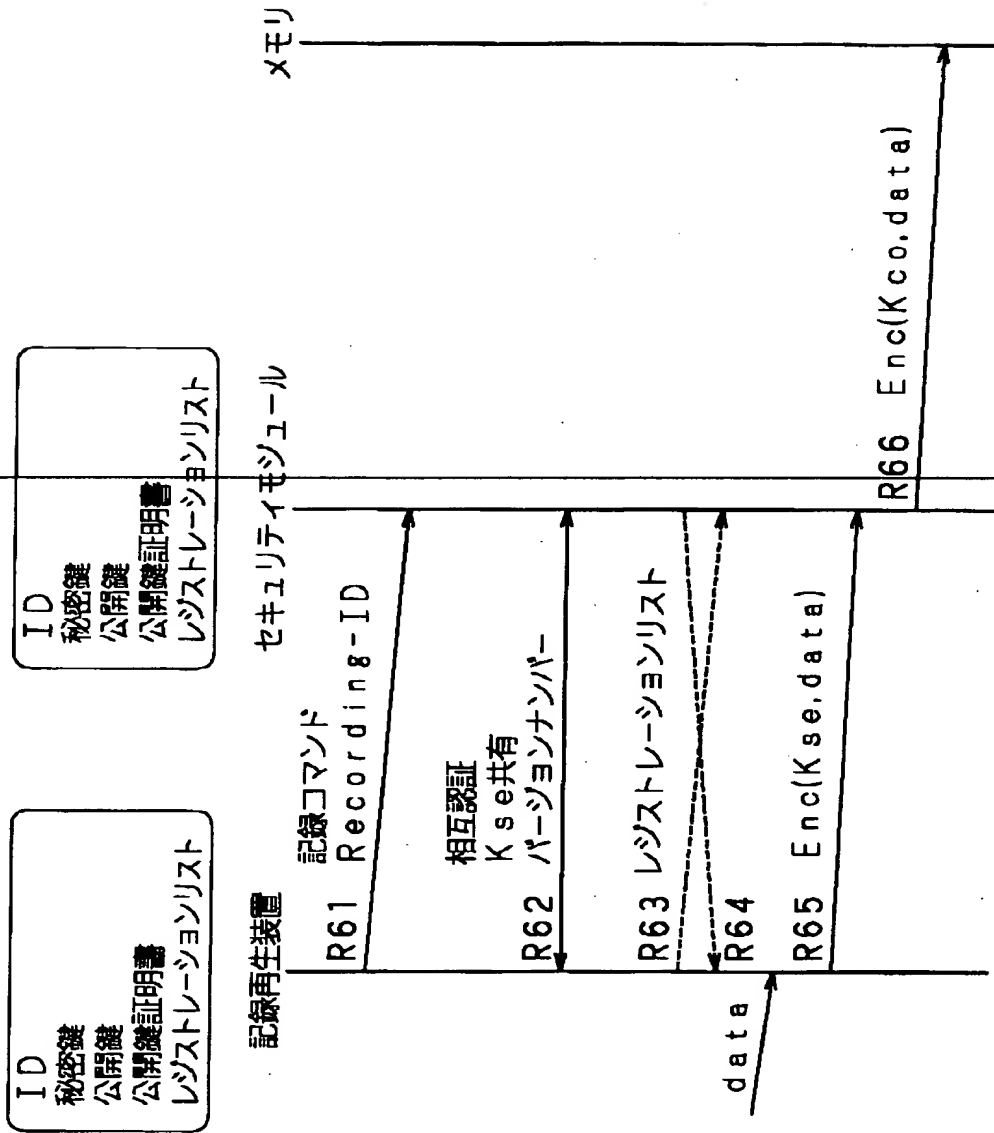
【図 3 1】



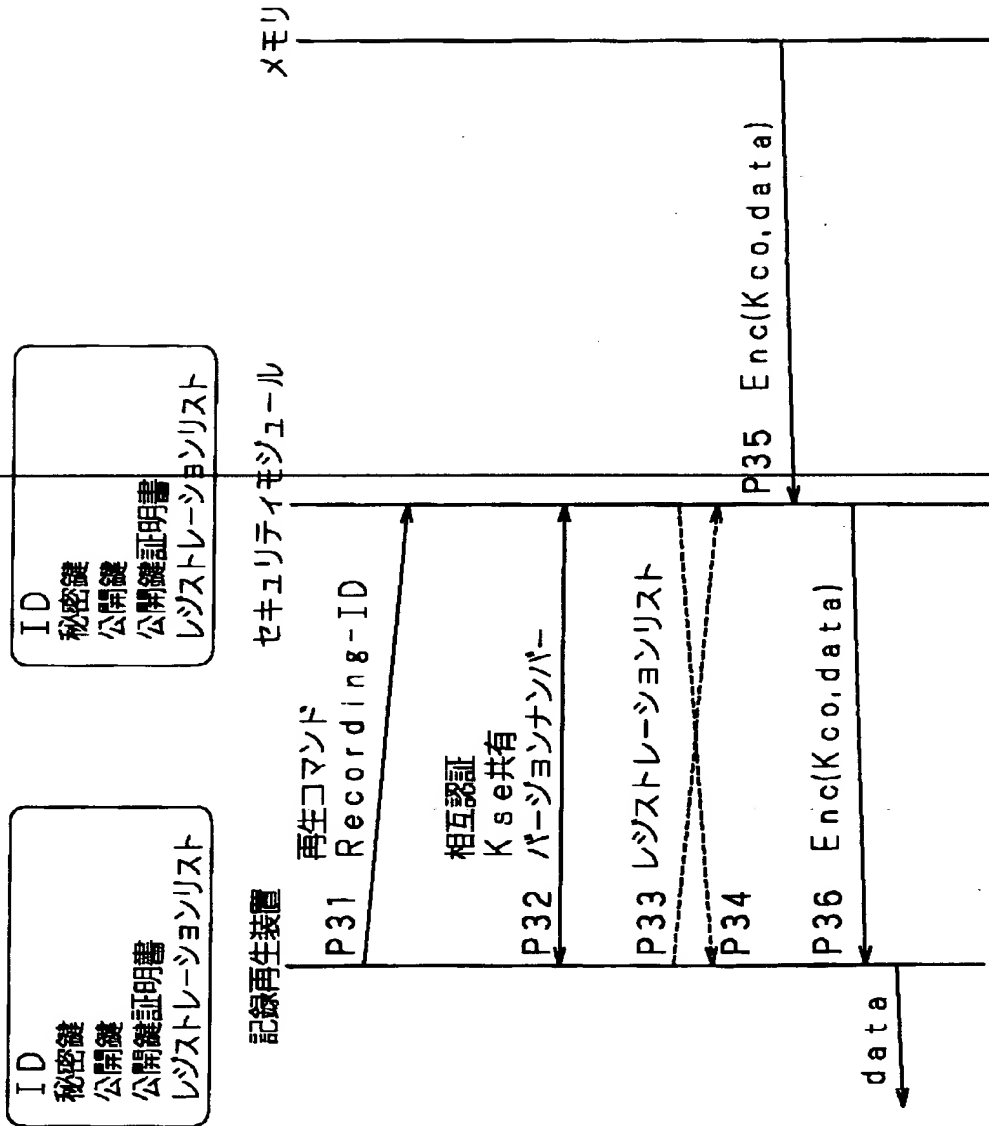
【図 3 2】



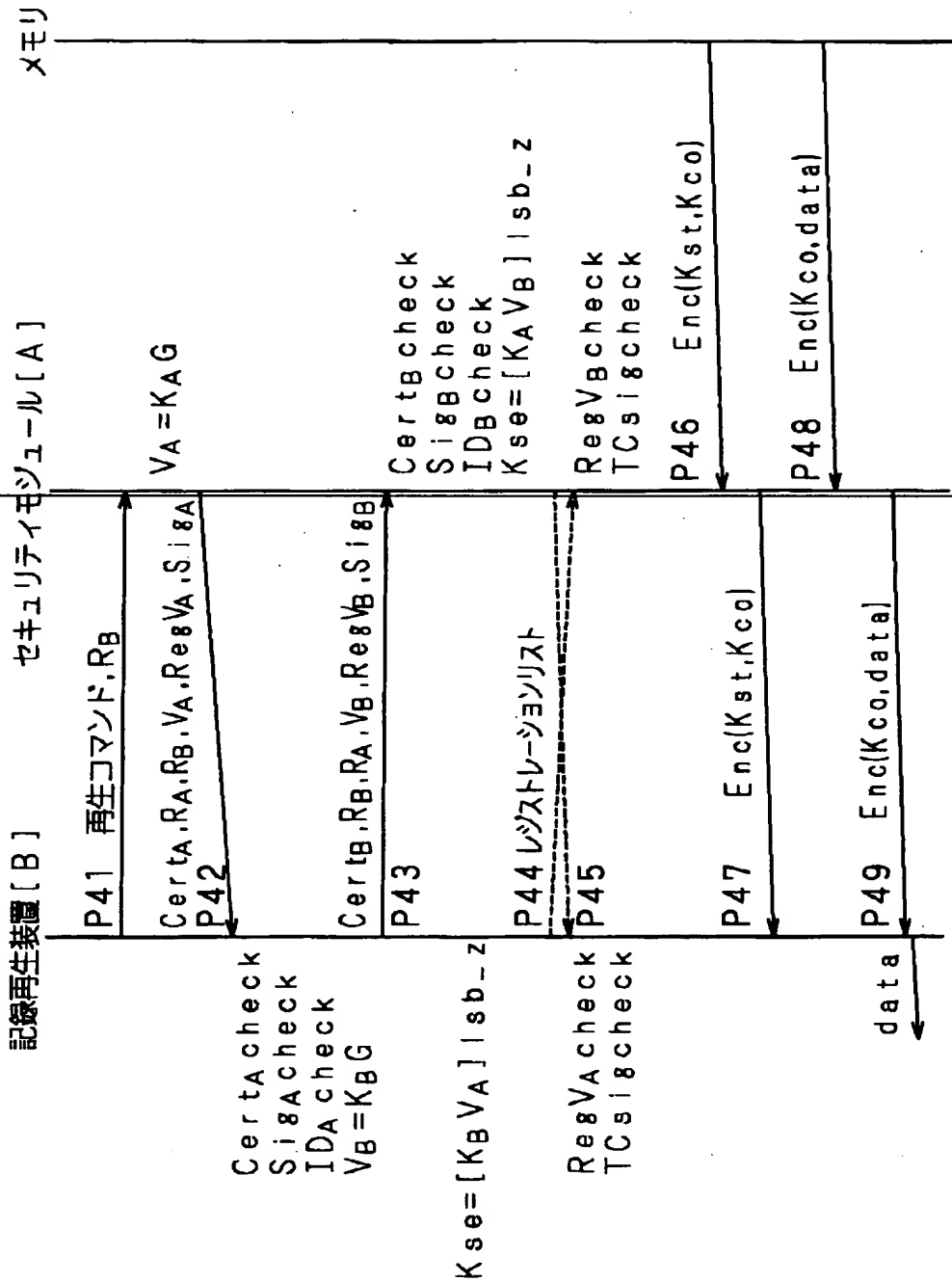
【図 3 3】



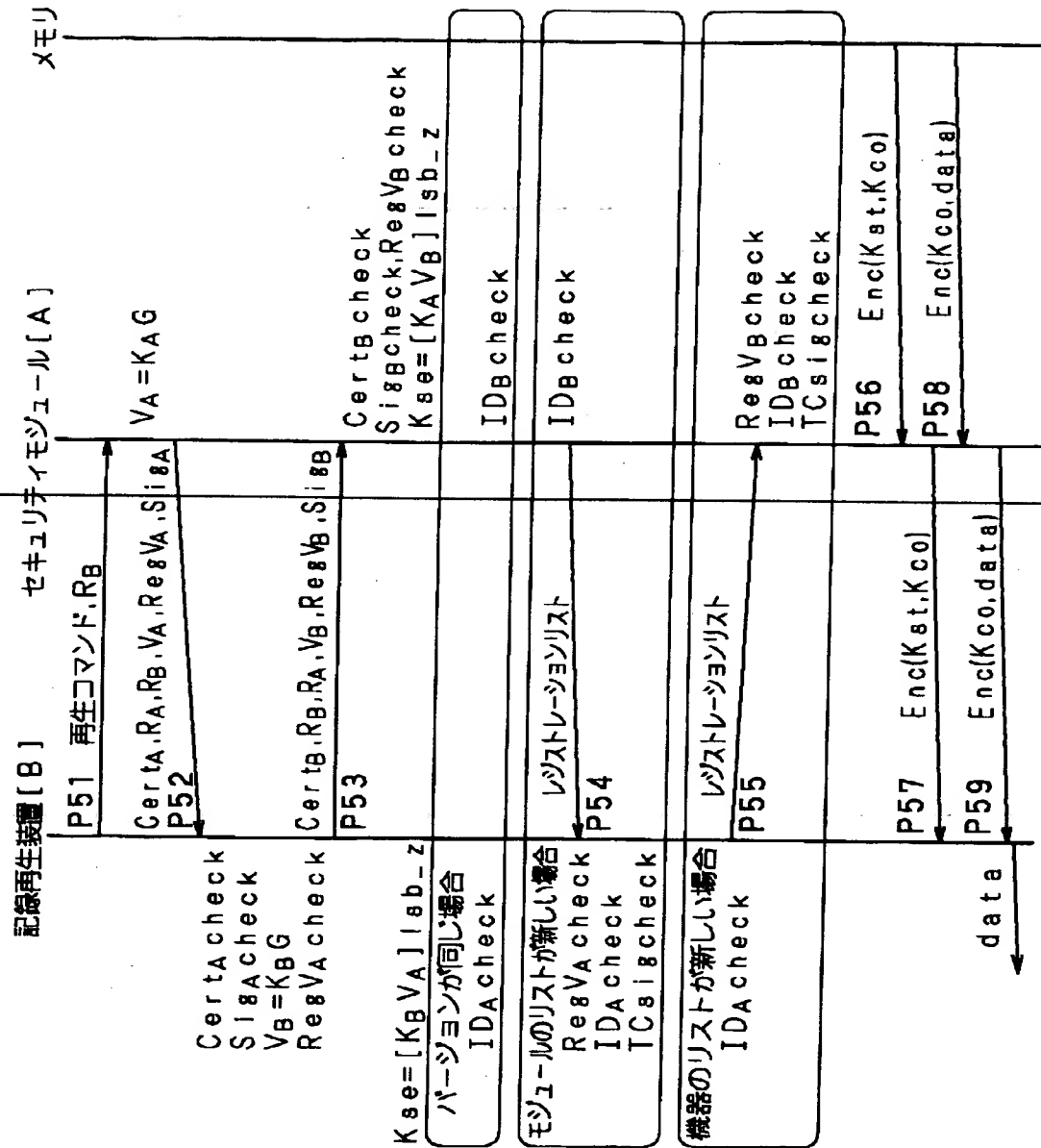
【図 3 4】



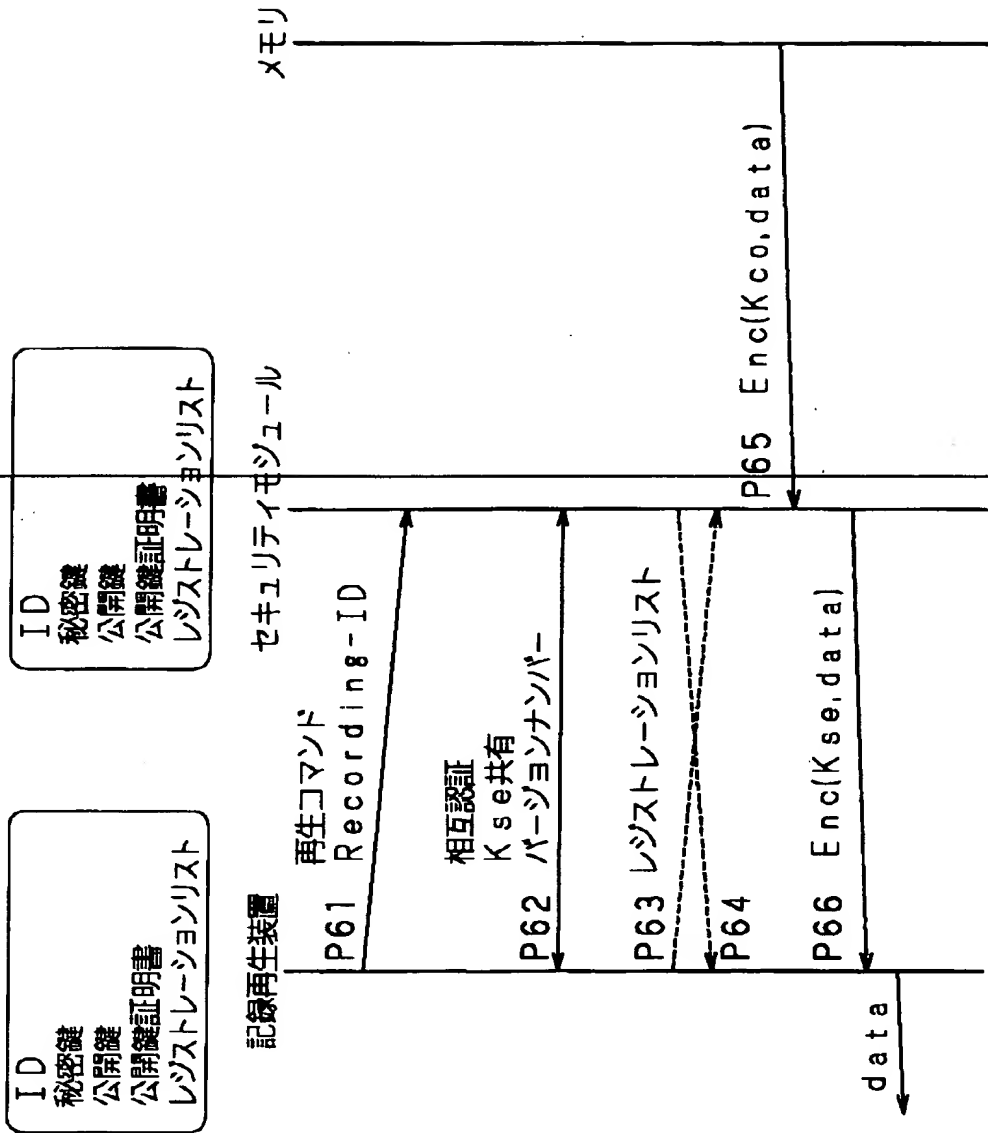
【図 3 5】



【図 3 6】



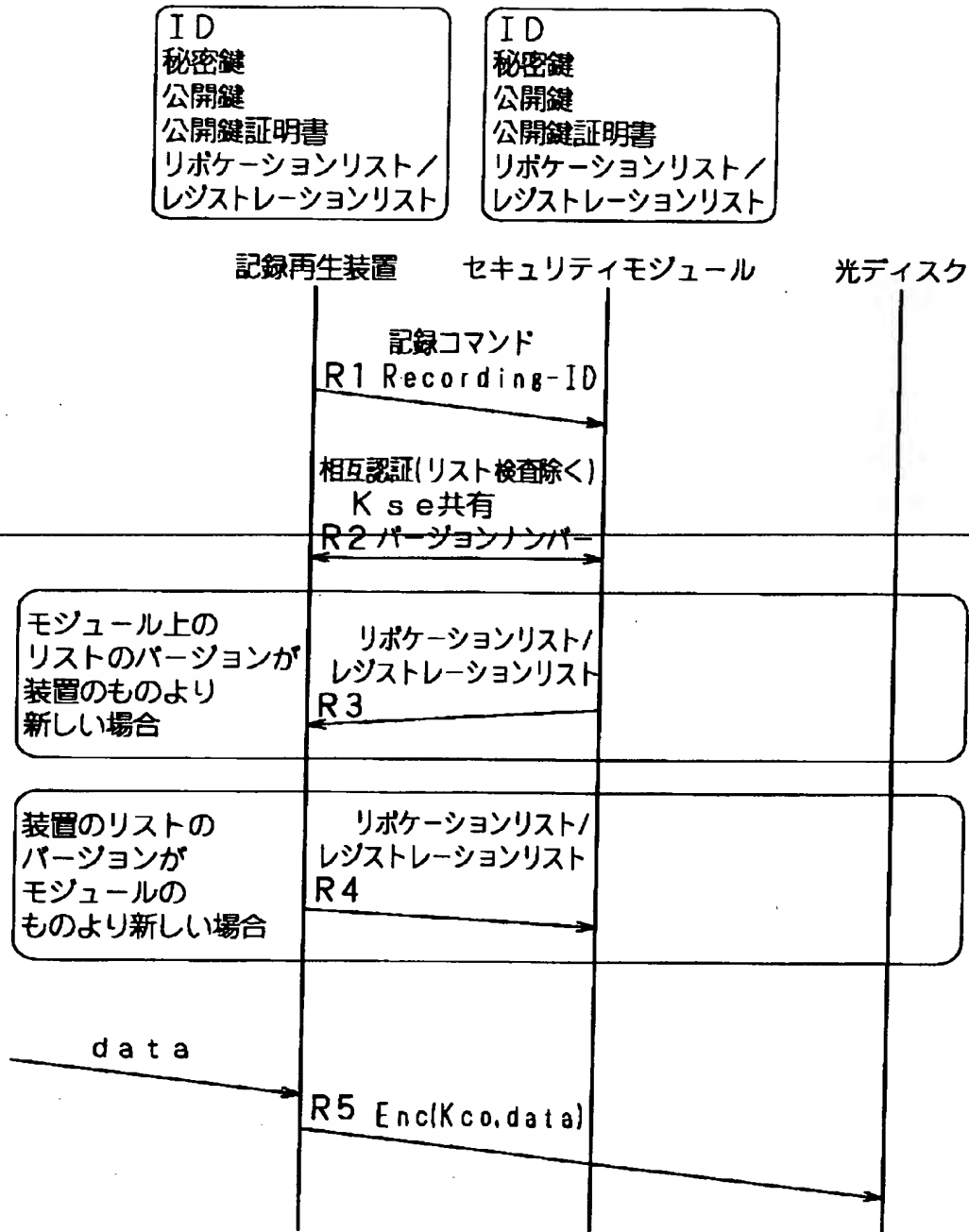
【図 3 7】



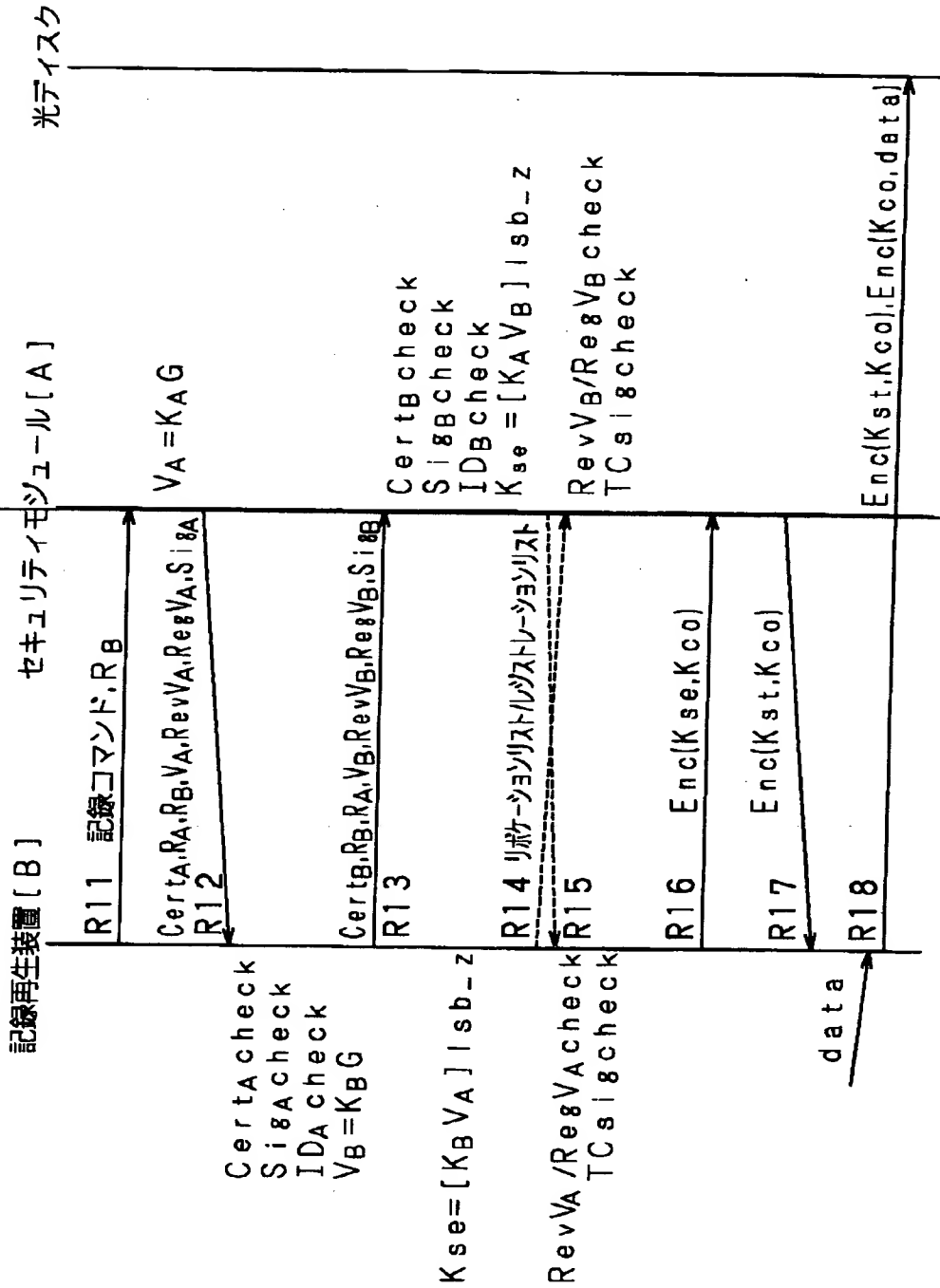
【図 3 8】

リポケーションリスト/レジストレーションリスト	
リポケーションリスト/レジストレーションリスト区別	
バージョンナンバー	
リポークされる機器または媒体の ID (リポケーションリスト), 登録される機器または媒体の ID (レジストレーションリスト)	
...	
T C のデジタル署名	

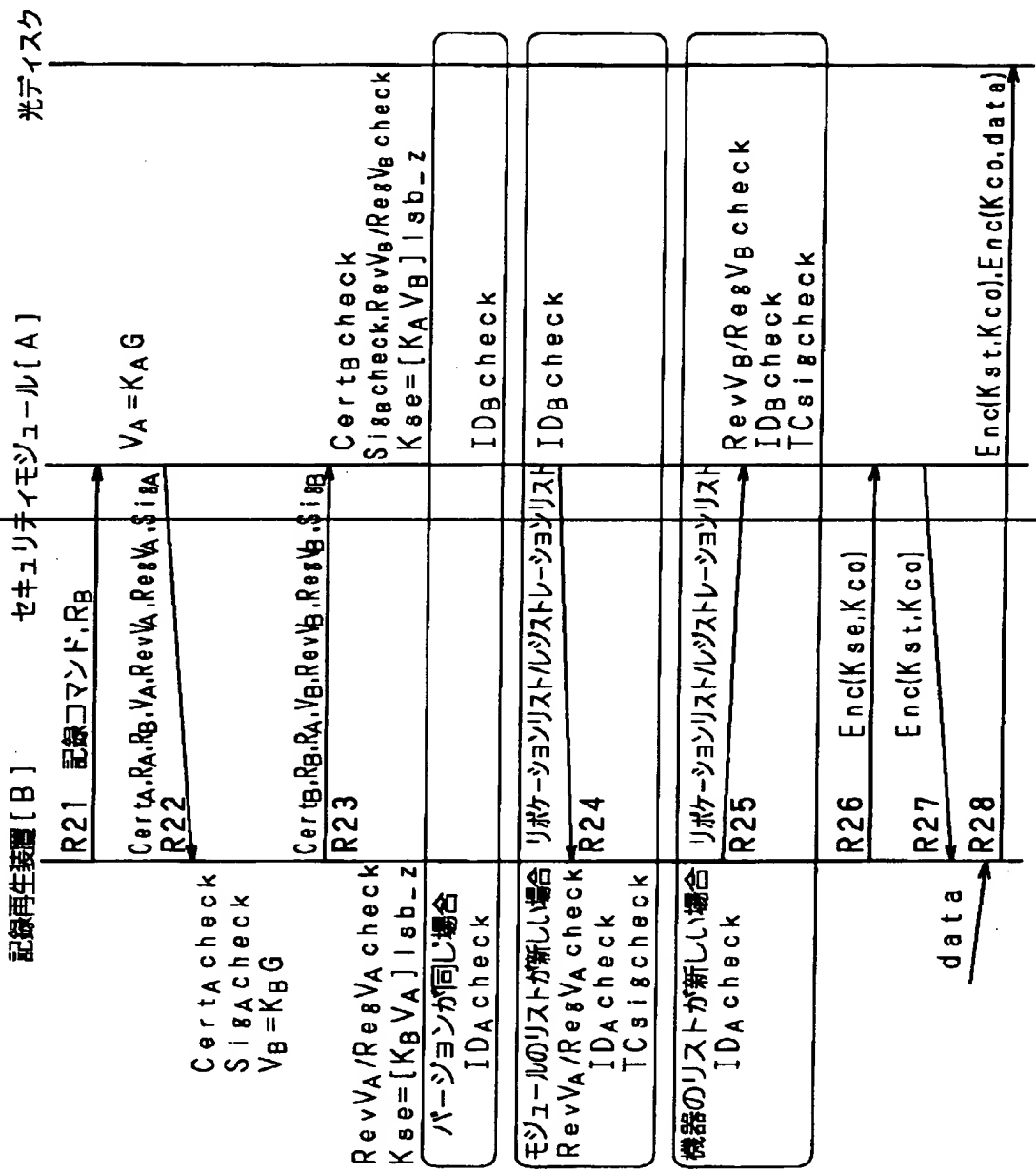
【図 3 9】



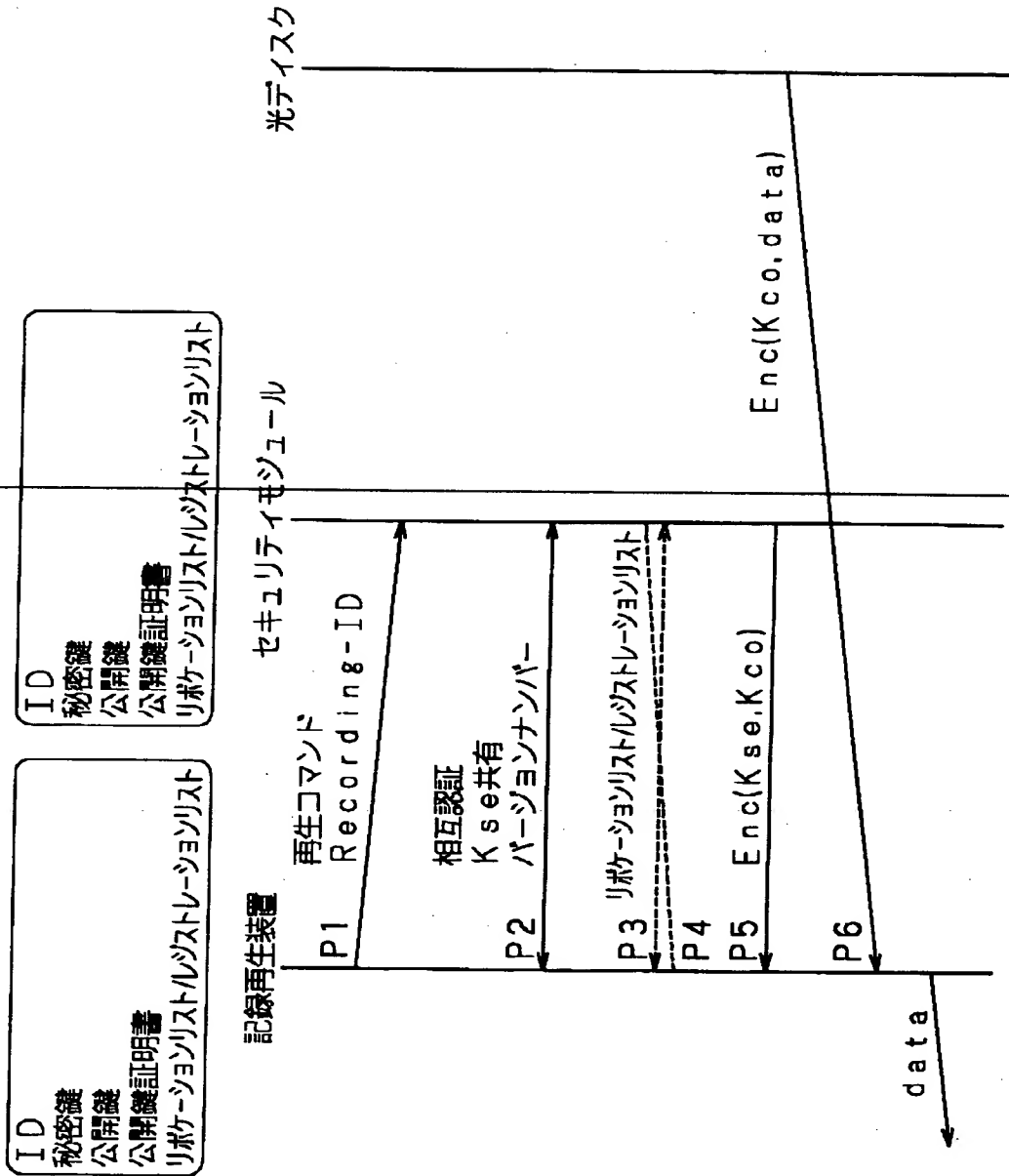
【図 4 0】



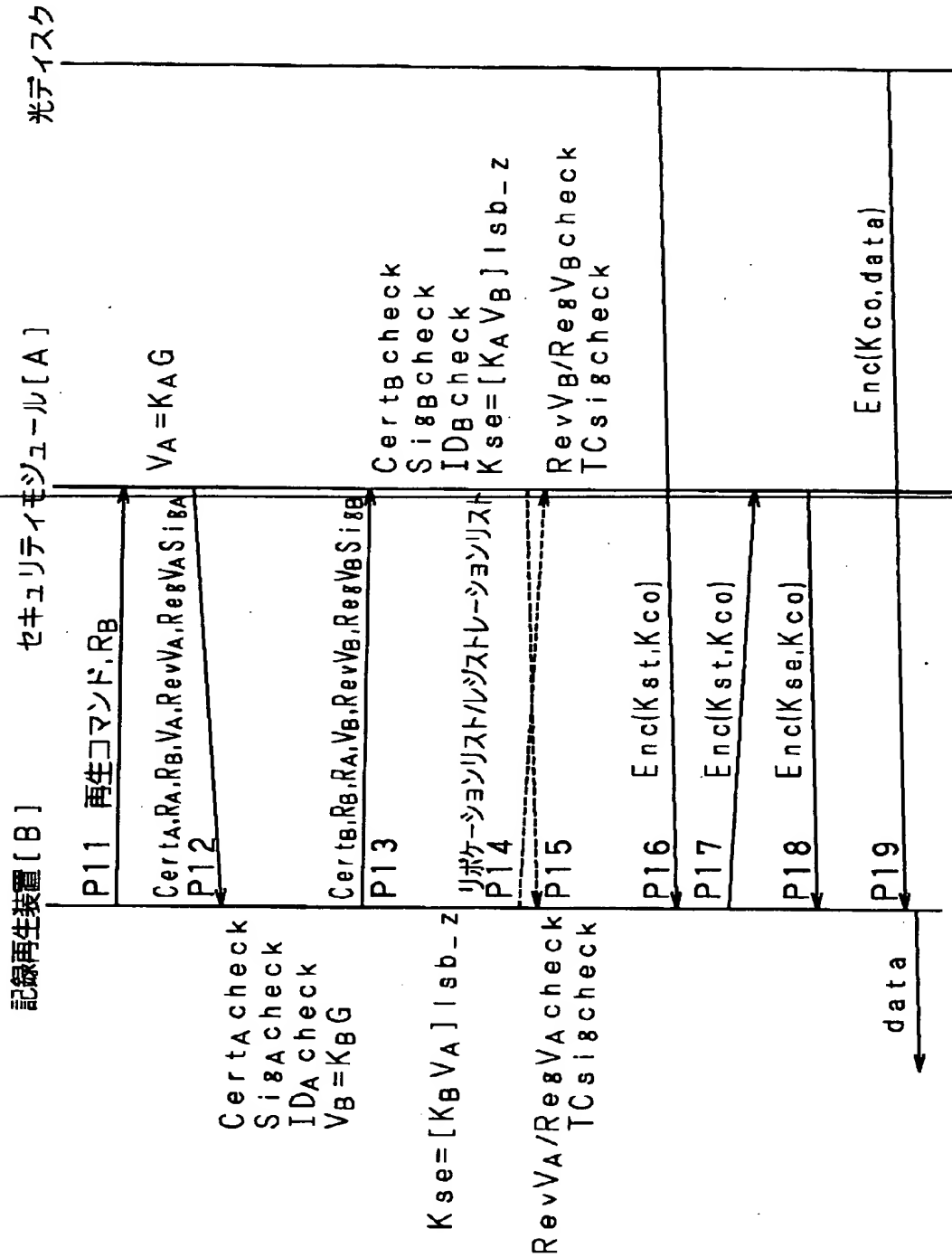
【図 4 1】



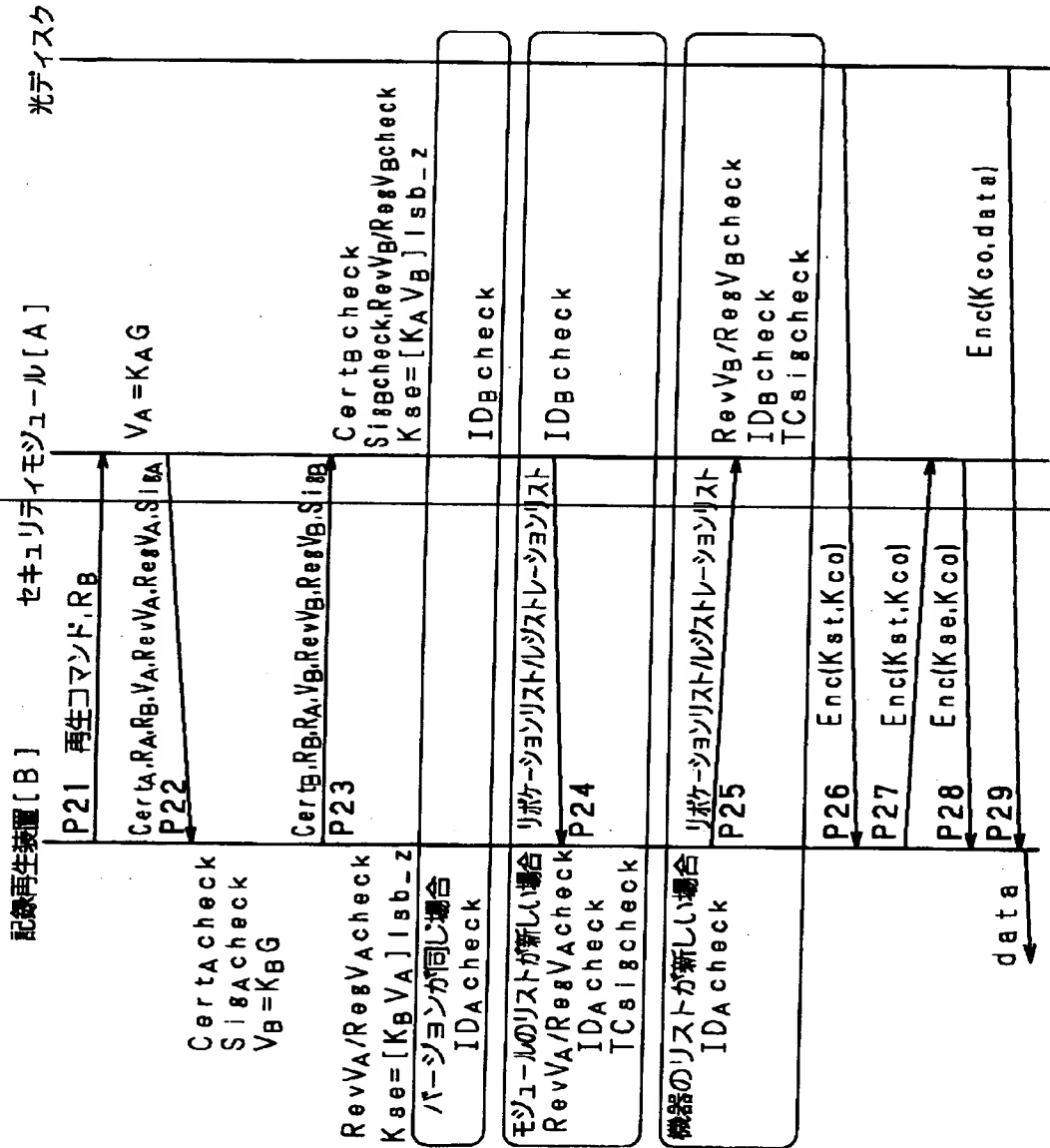
【図 4 2】



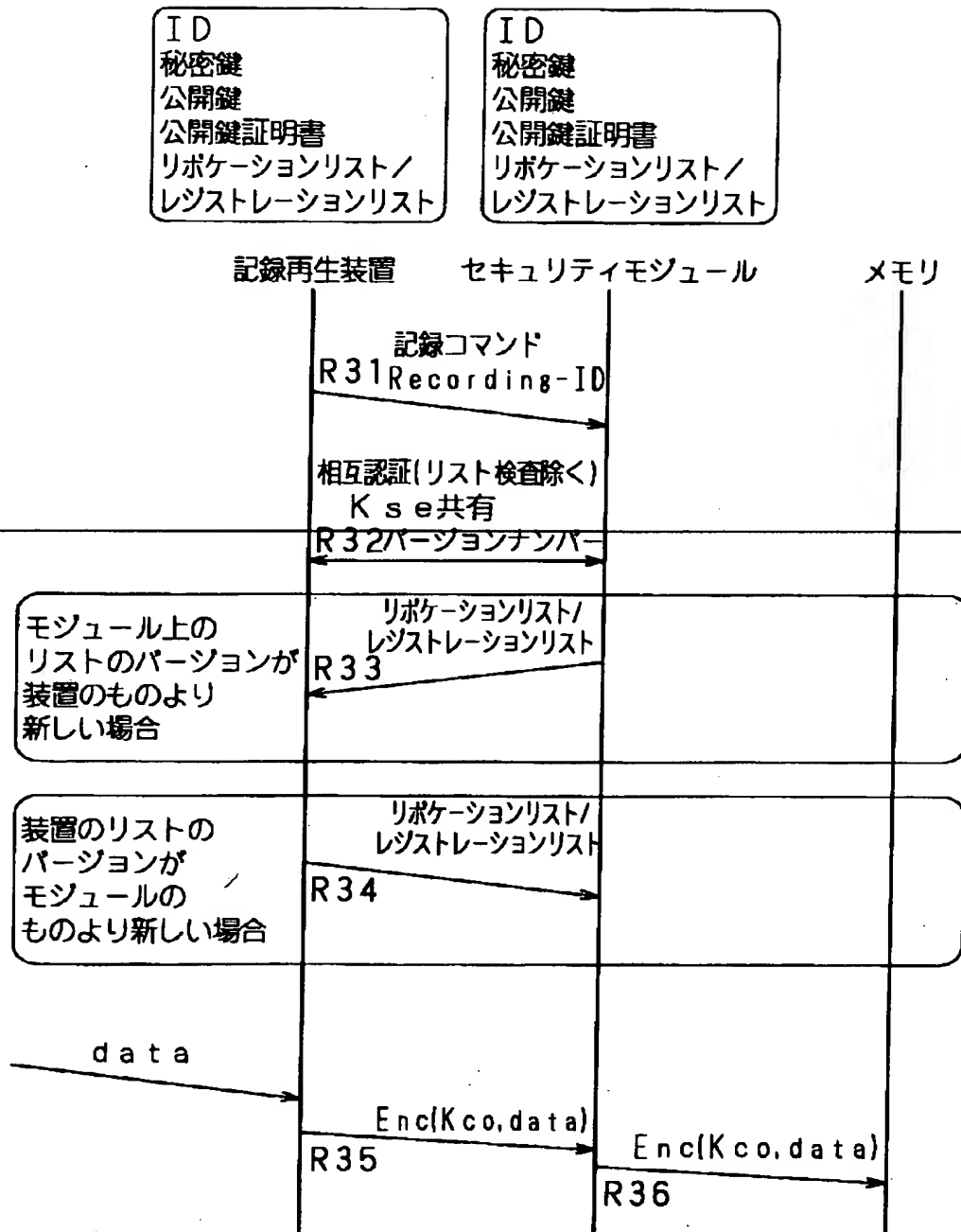
【図 4 3】



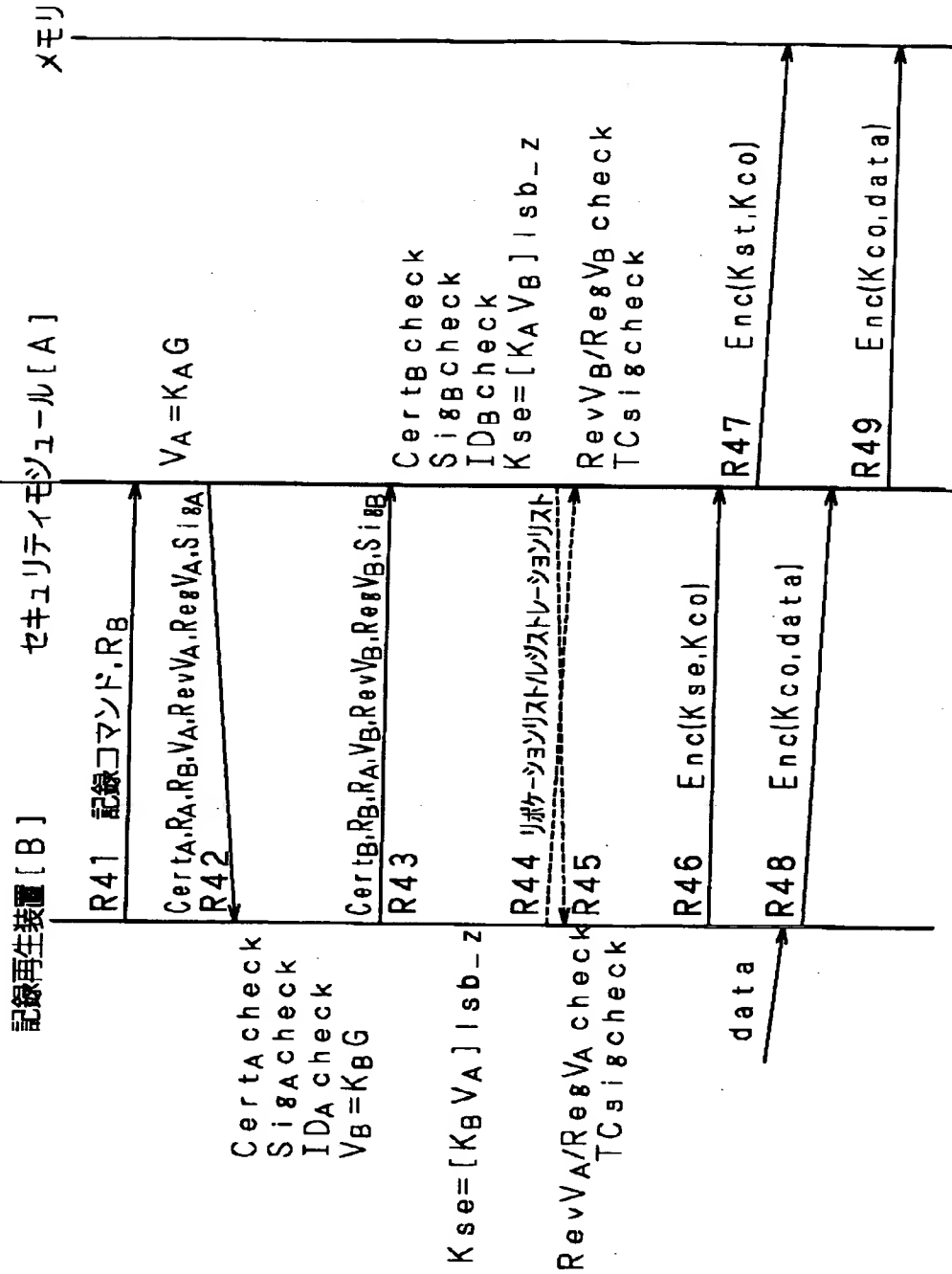
【図 44】



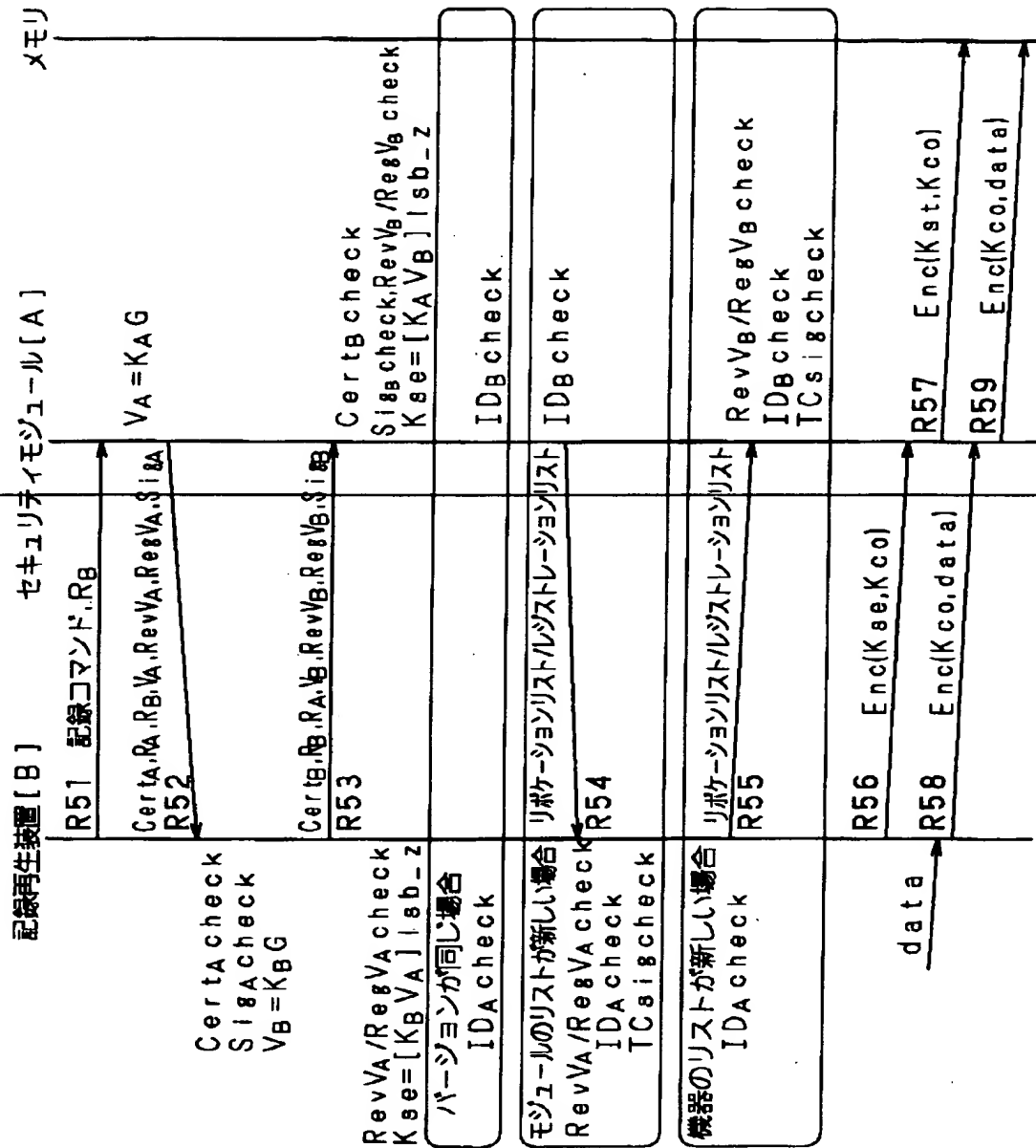
【図 4 5】



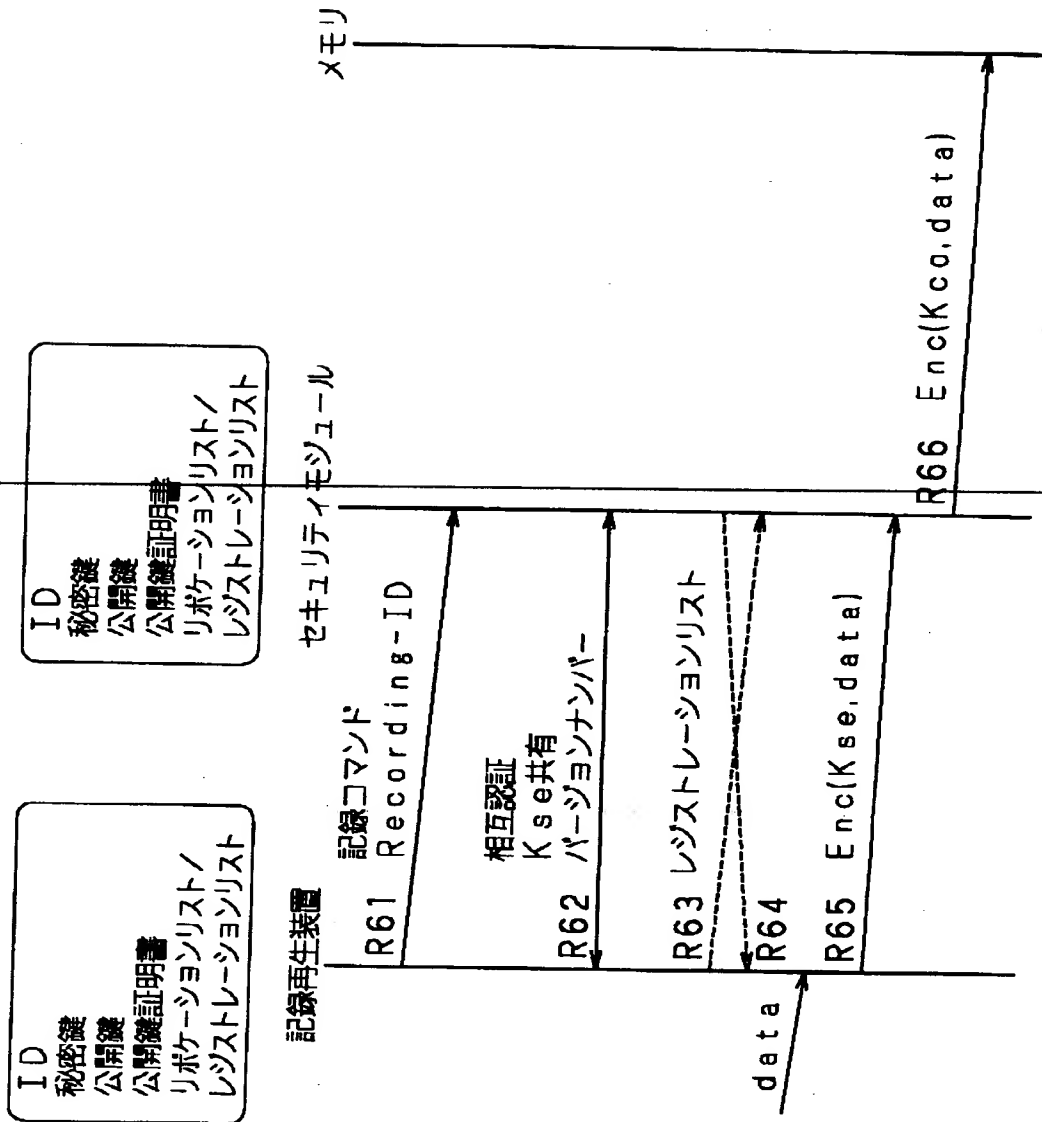
【図 4 6】



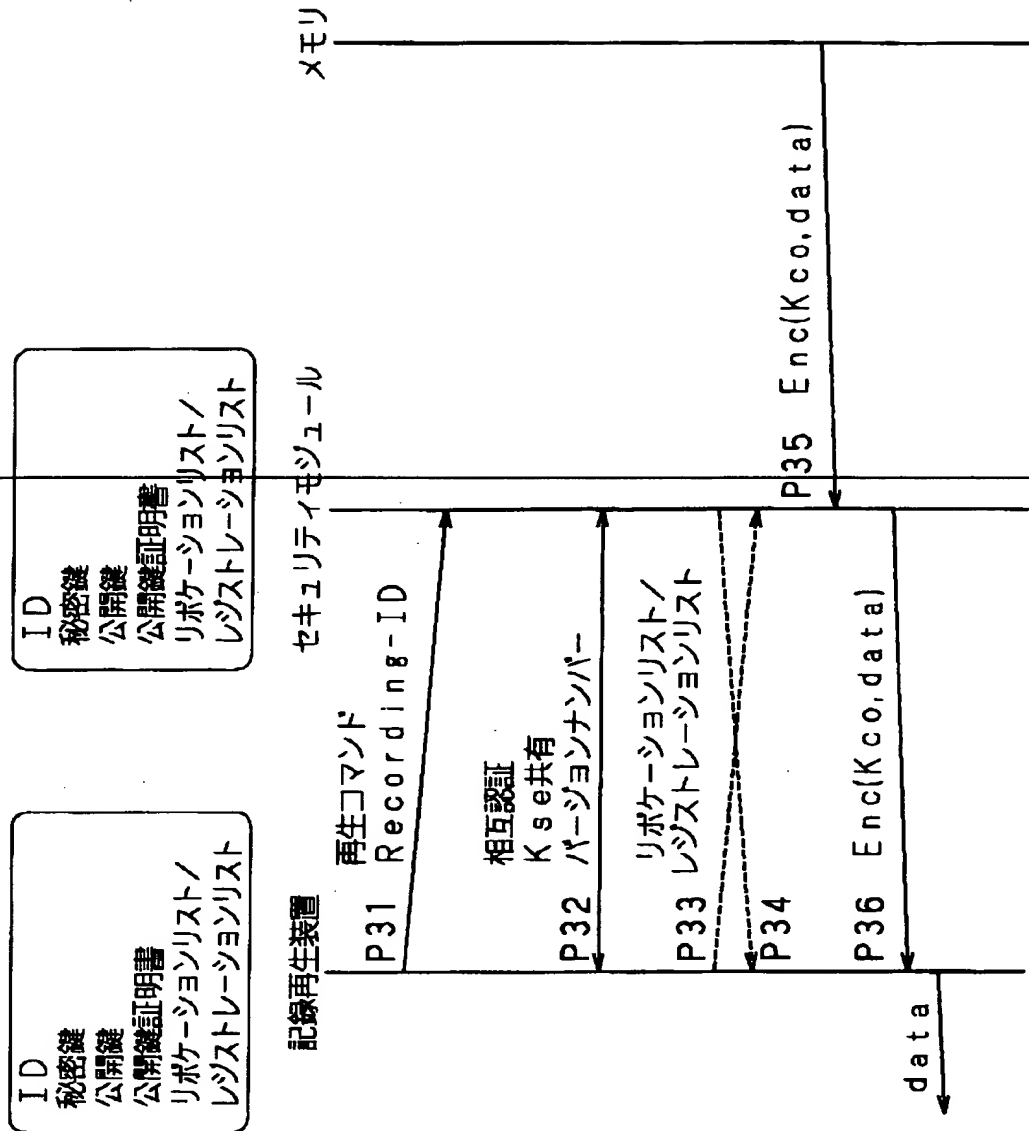
【図 4 7】



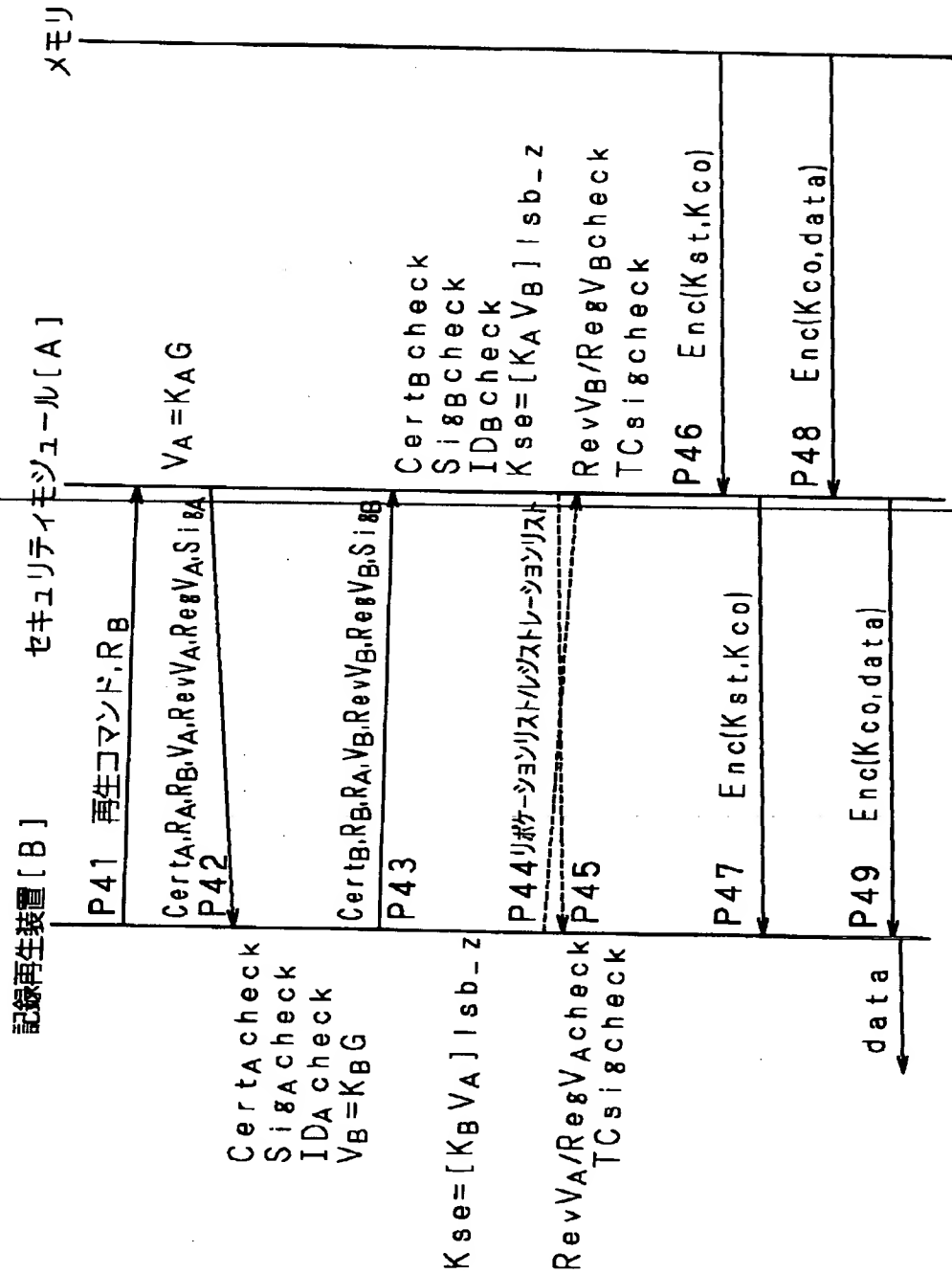
【図 4 8】



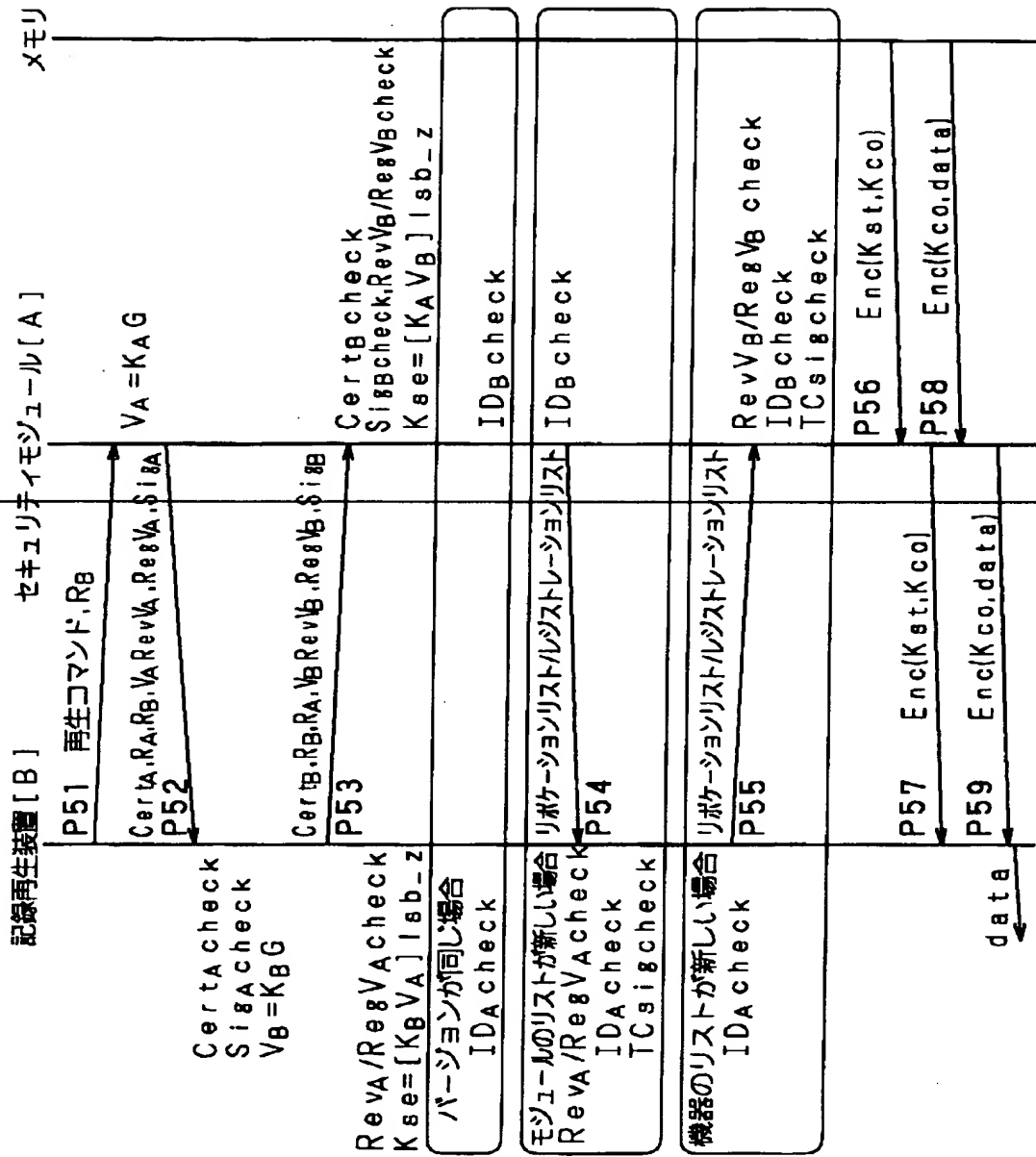
【図 4 9】



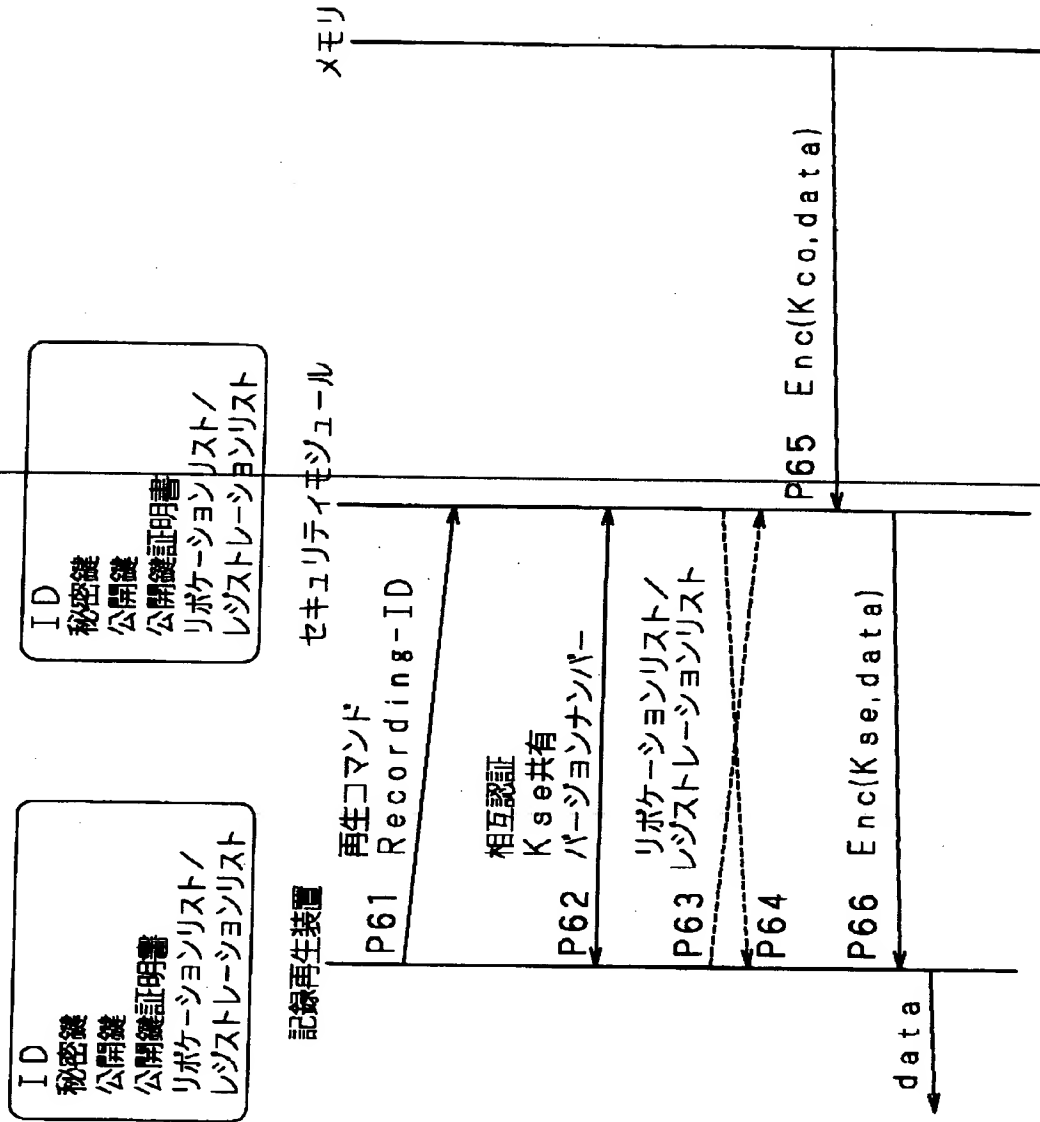
【図 5 0】



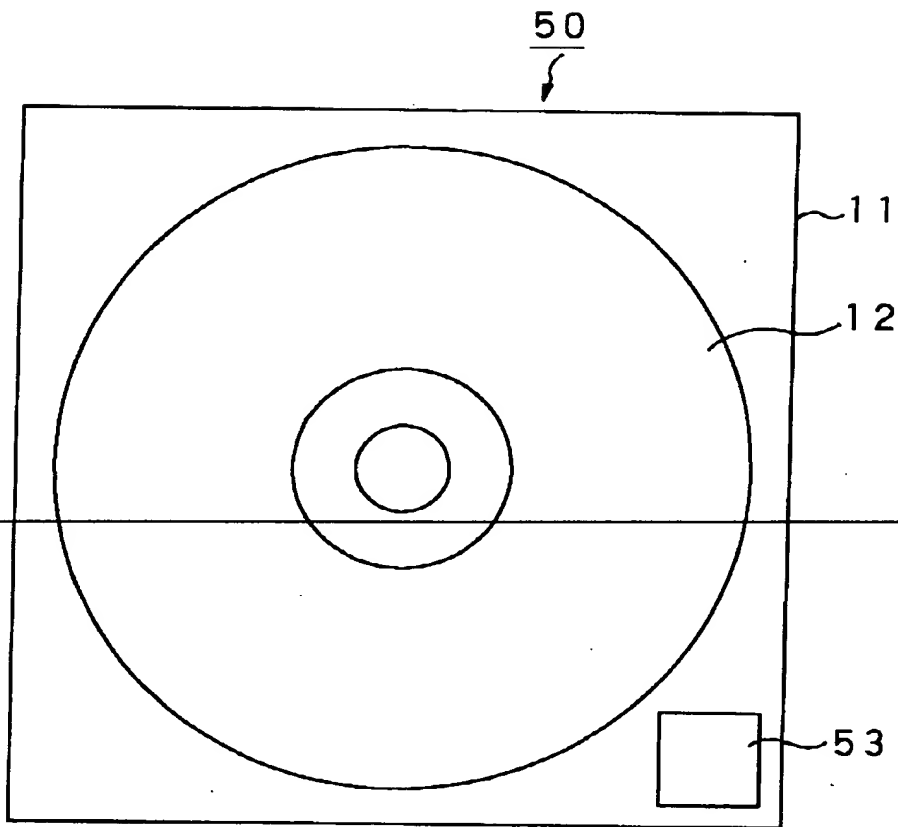
【図 5 1】



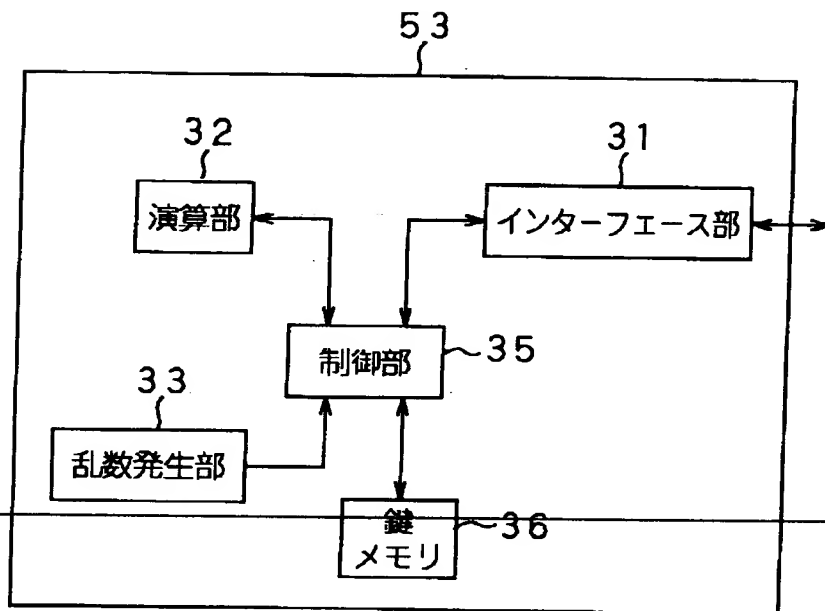
【図 5 2】



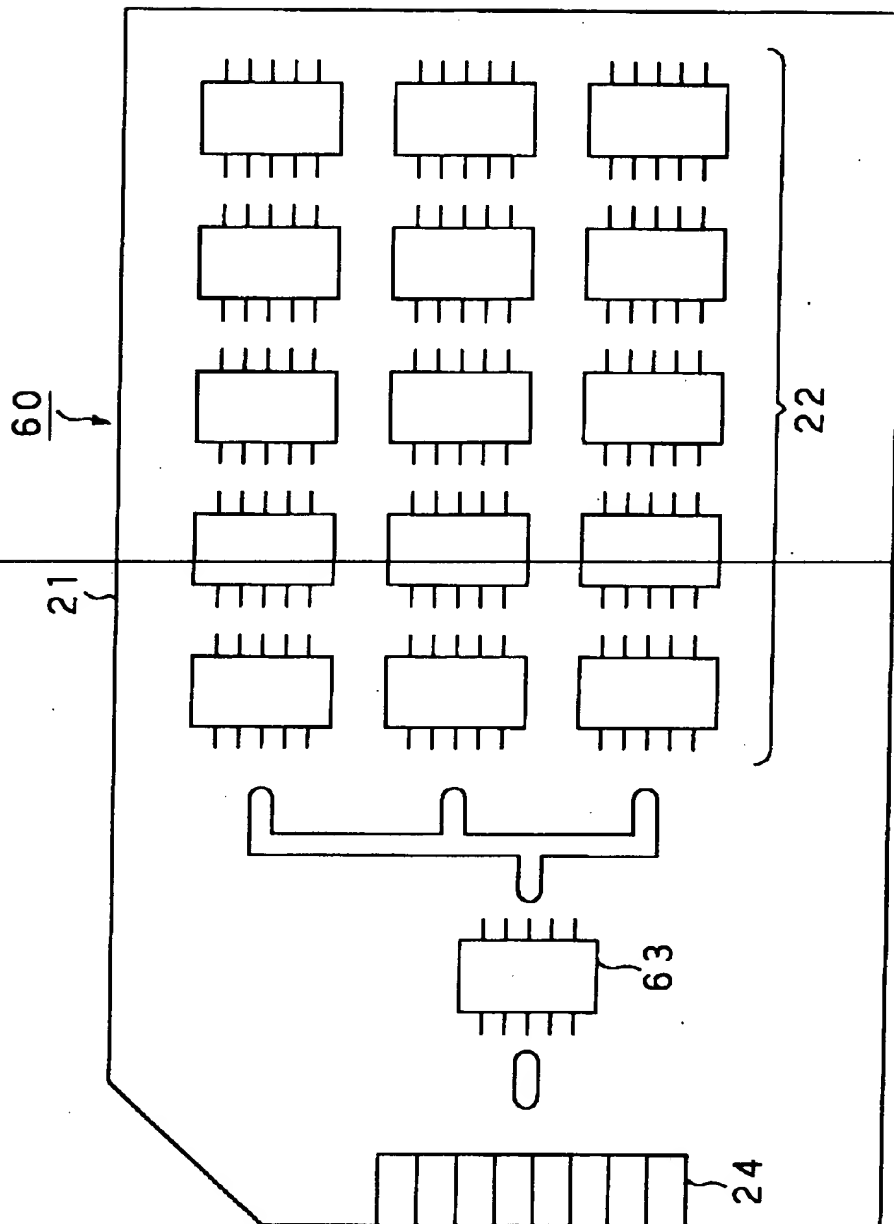
【図 53】



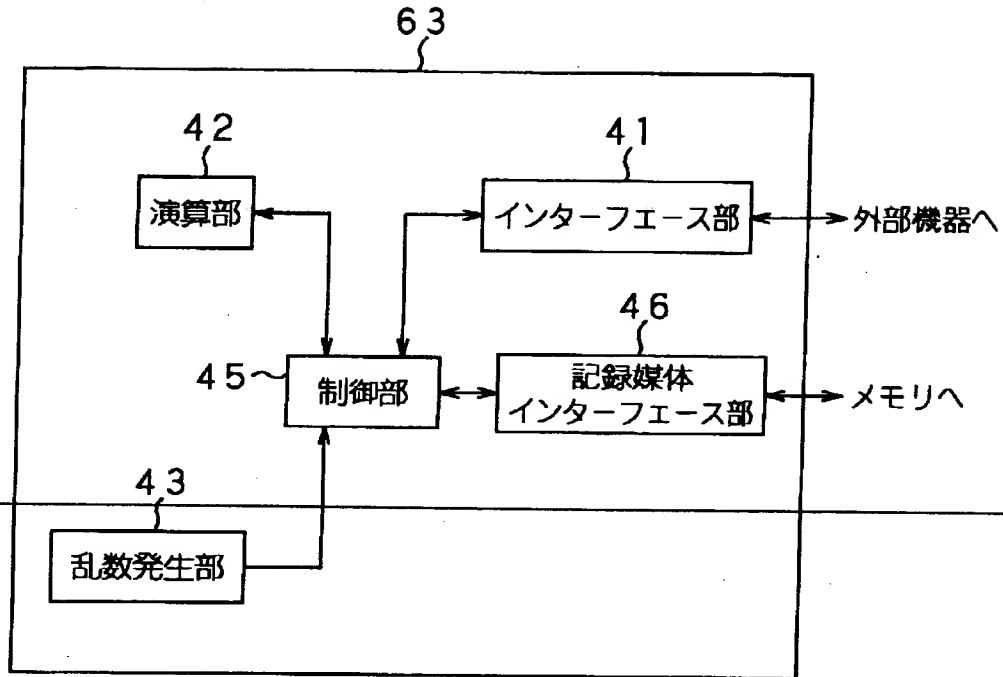
【図 5 4】



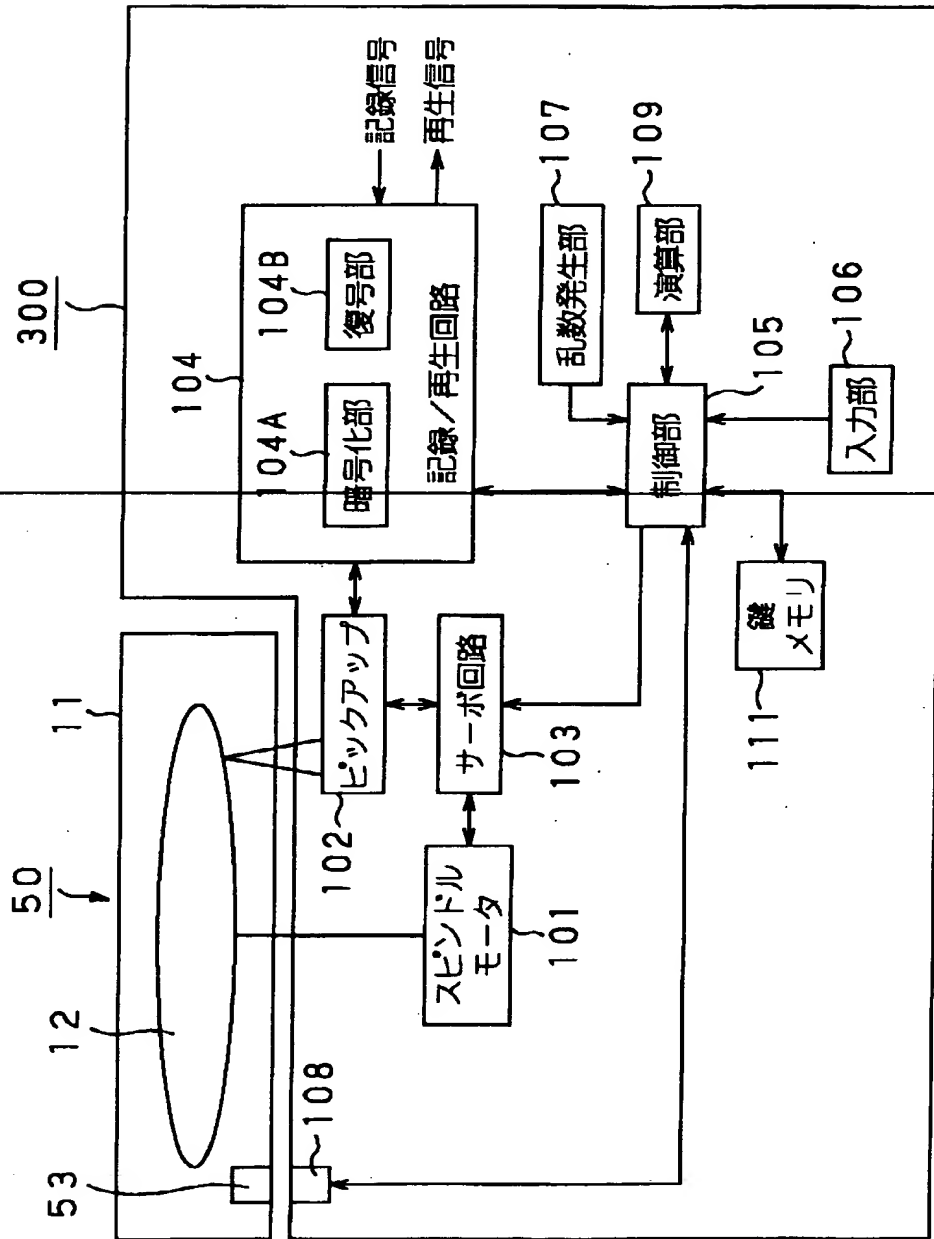
【図 5 5】



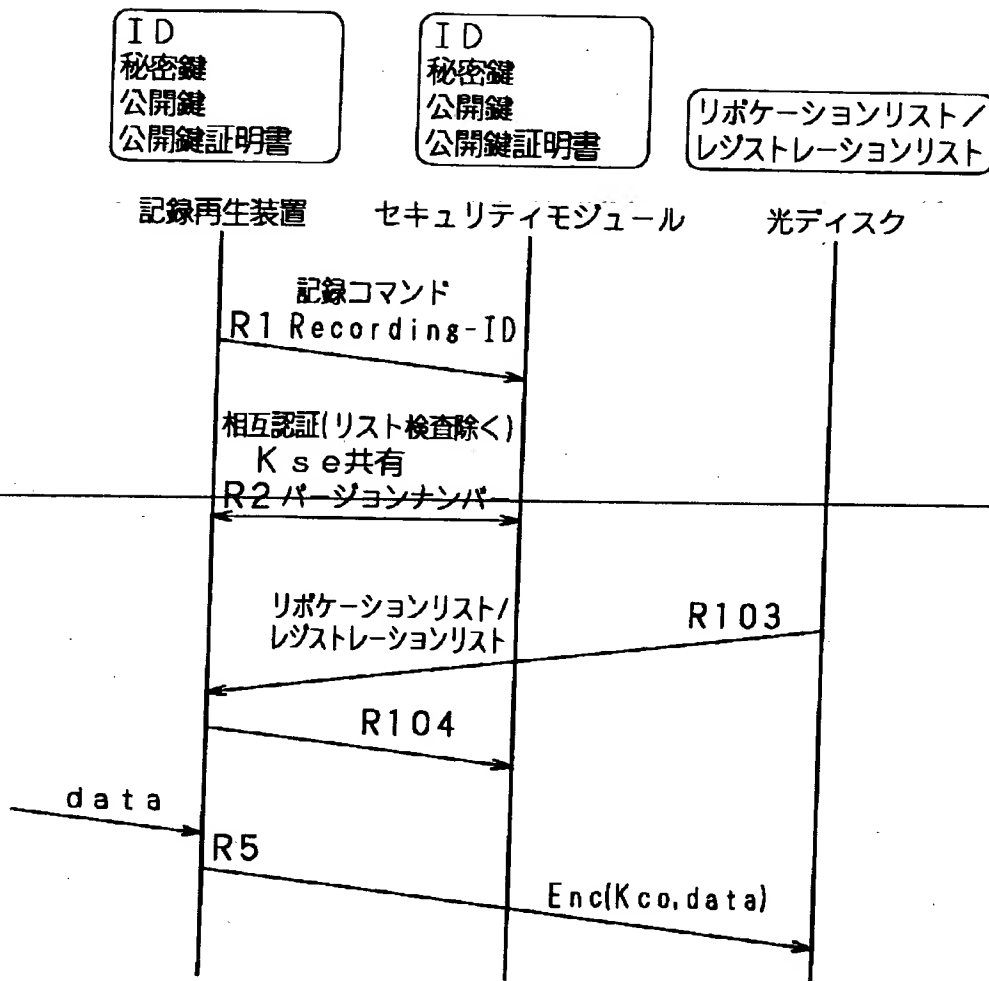
【図 5 6】



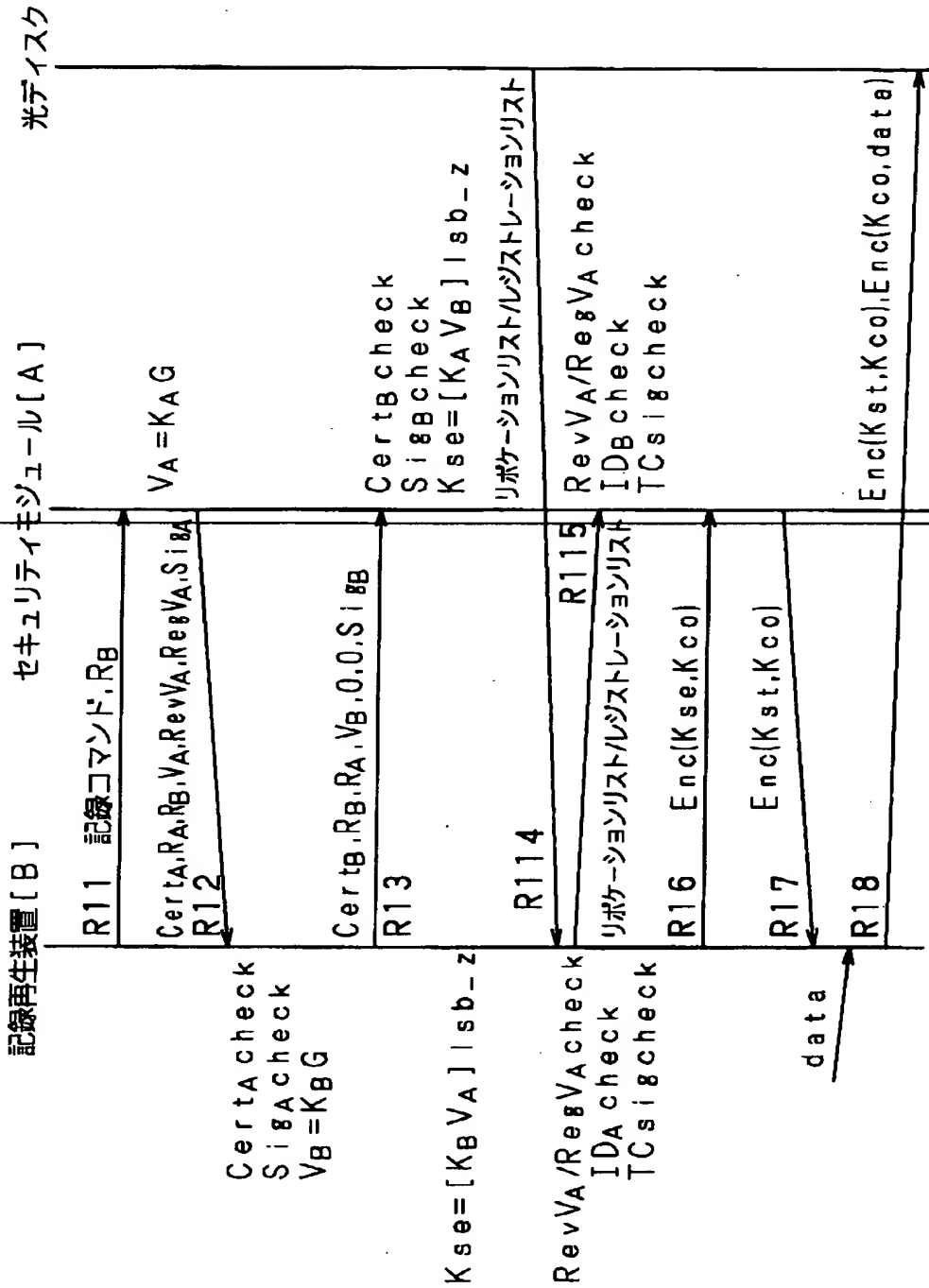
【図 5 7】



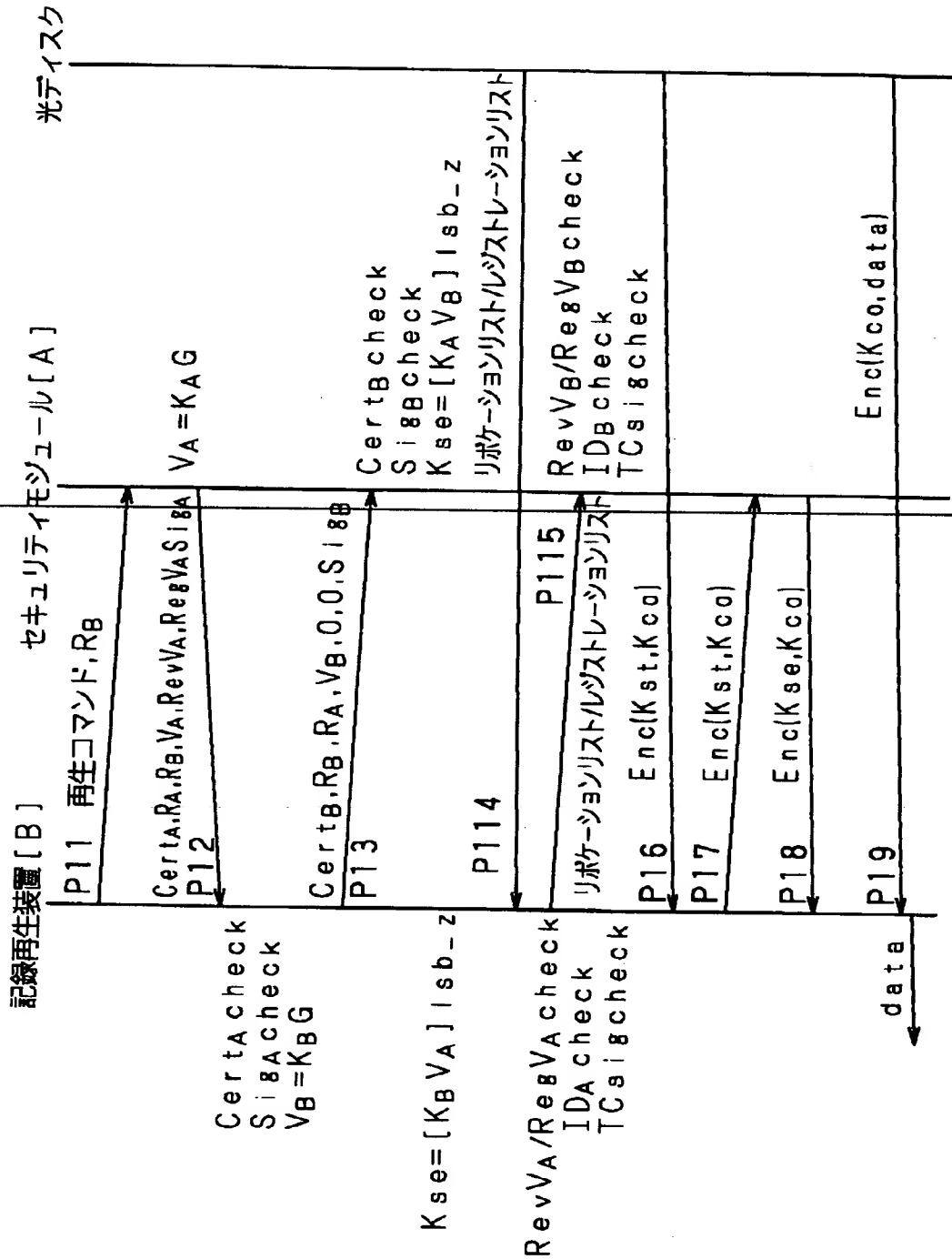
【図 5 8】



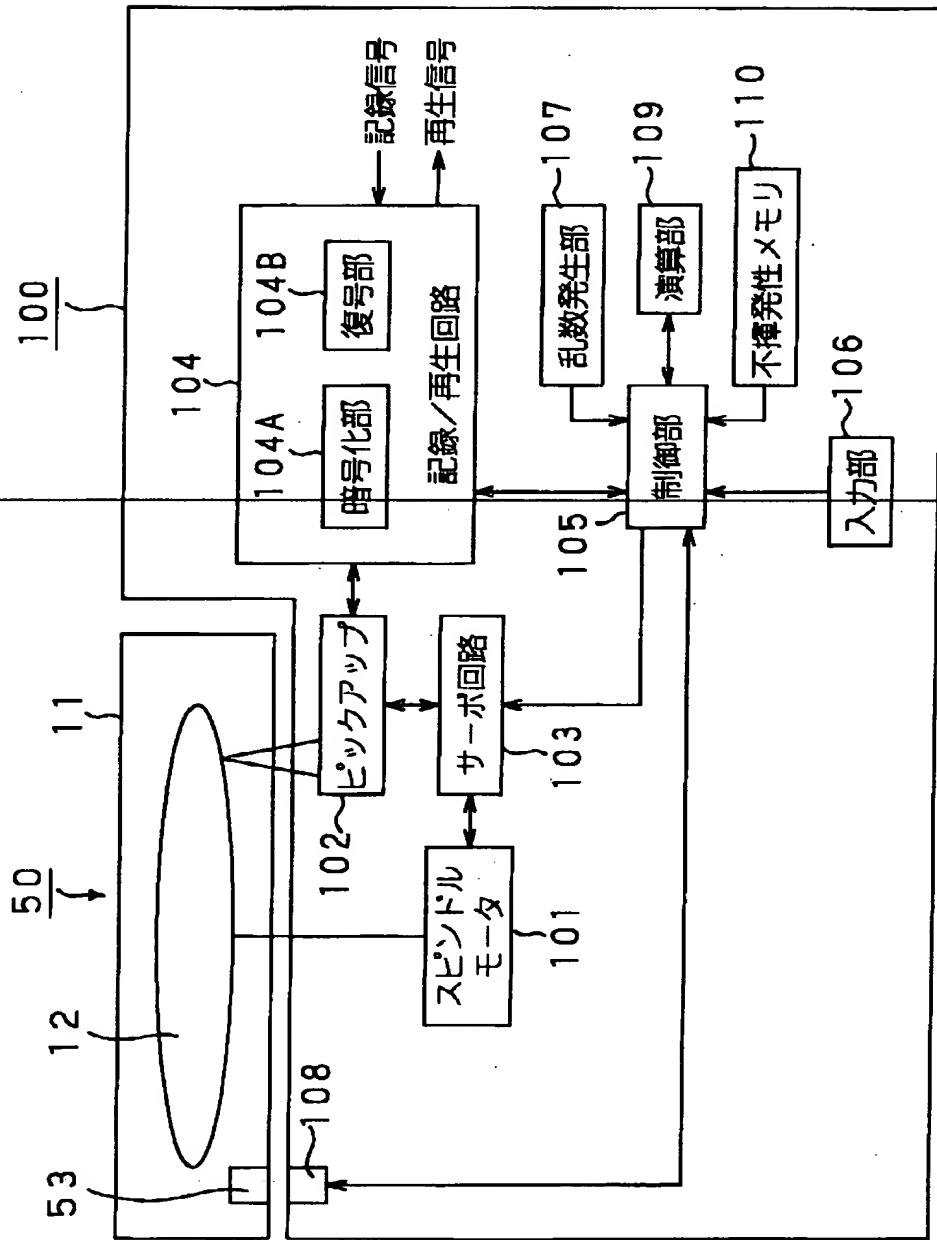
【図 5 9】



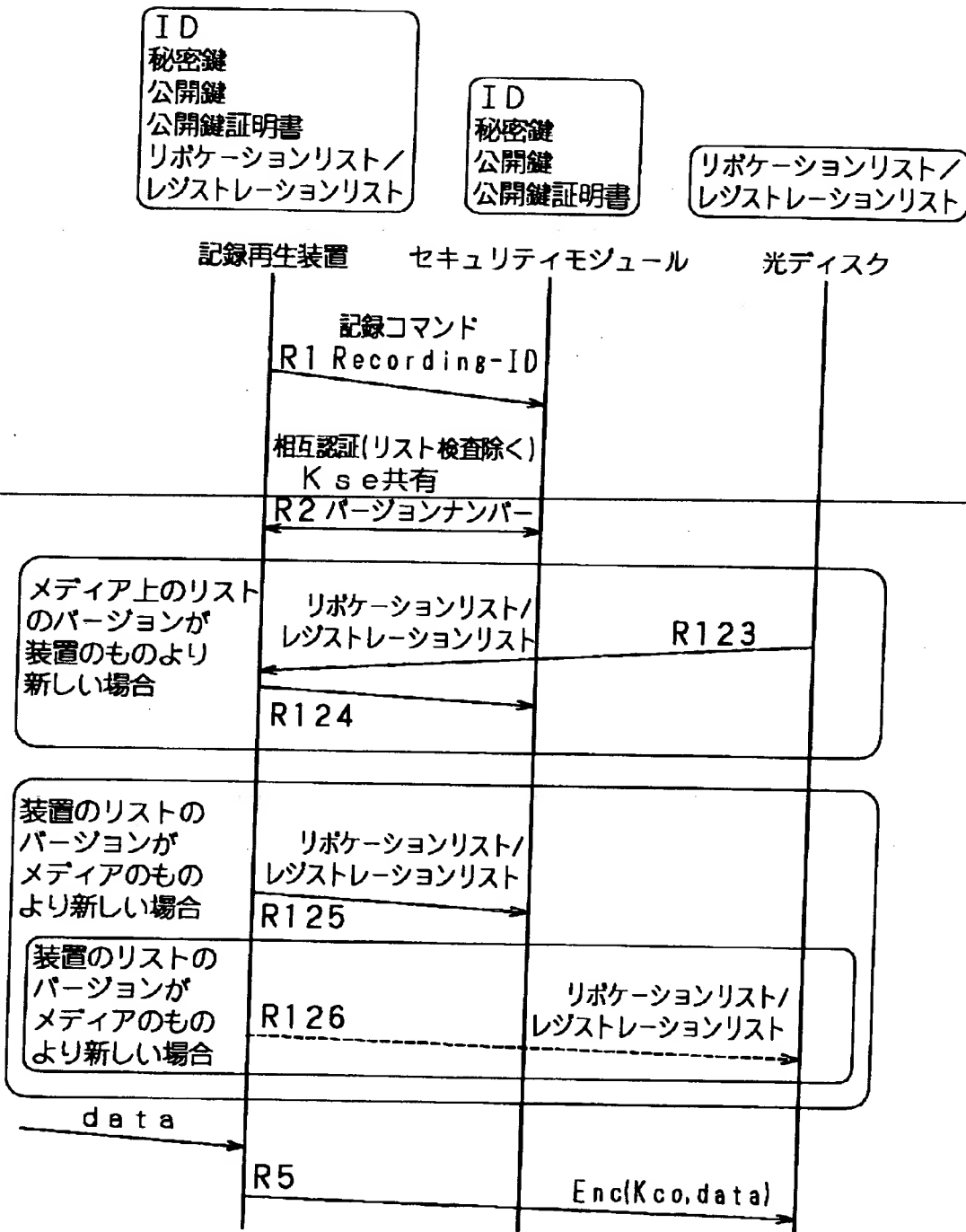
【図 6 0】



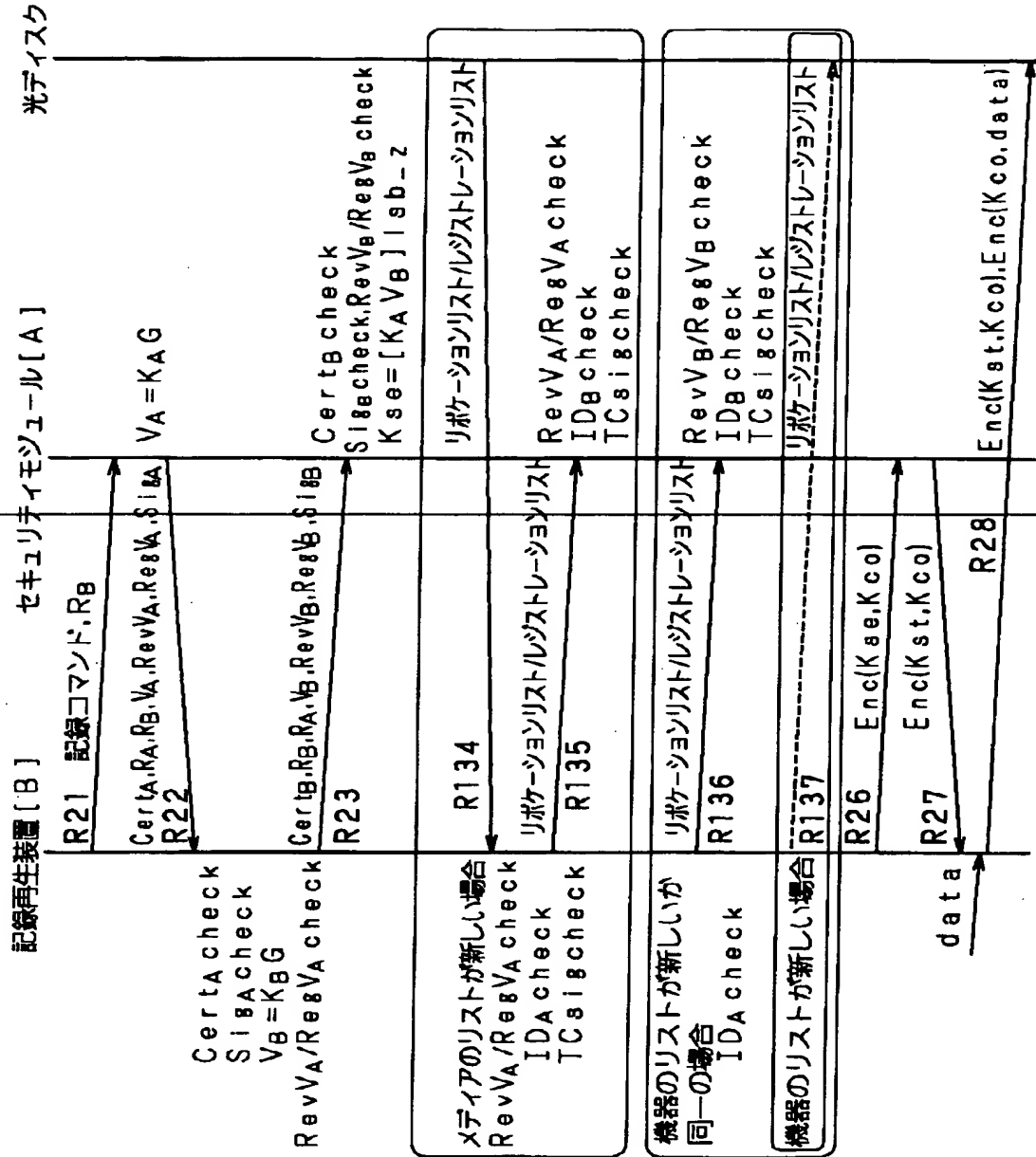
【図 6 1】



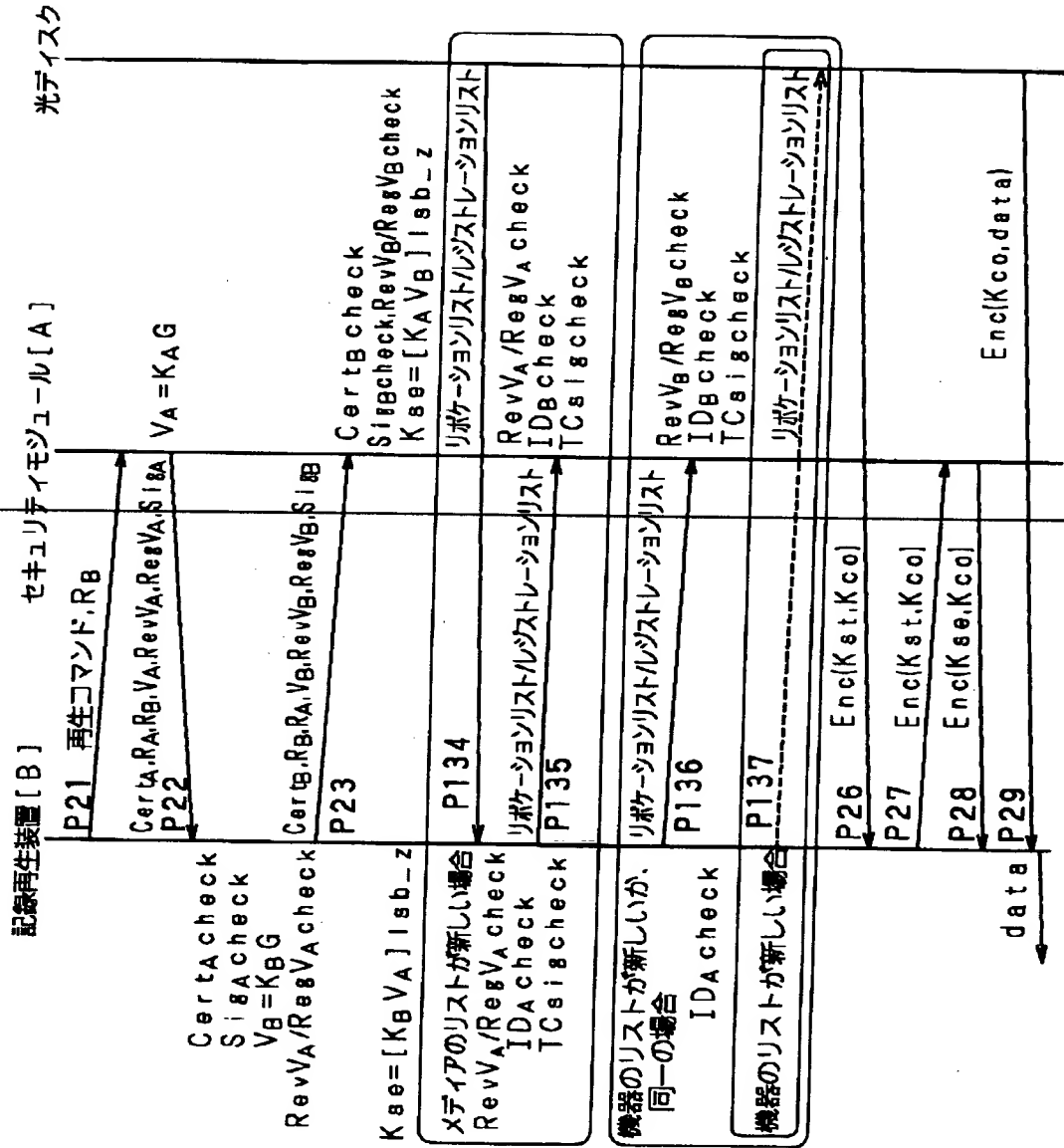
【図 6 2】



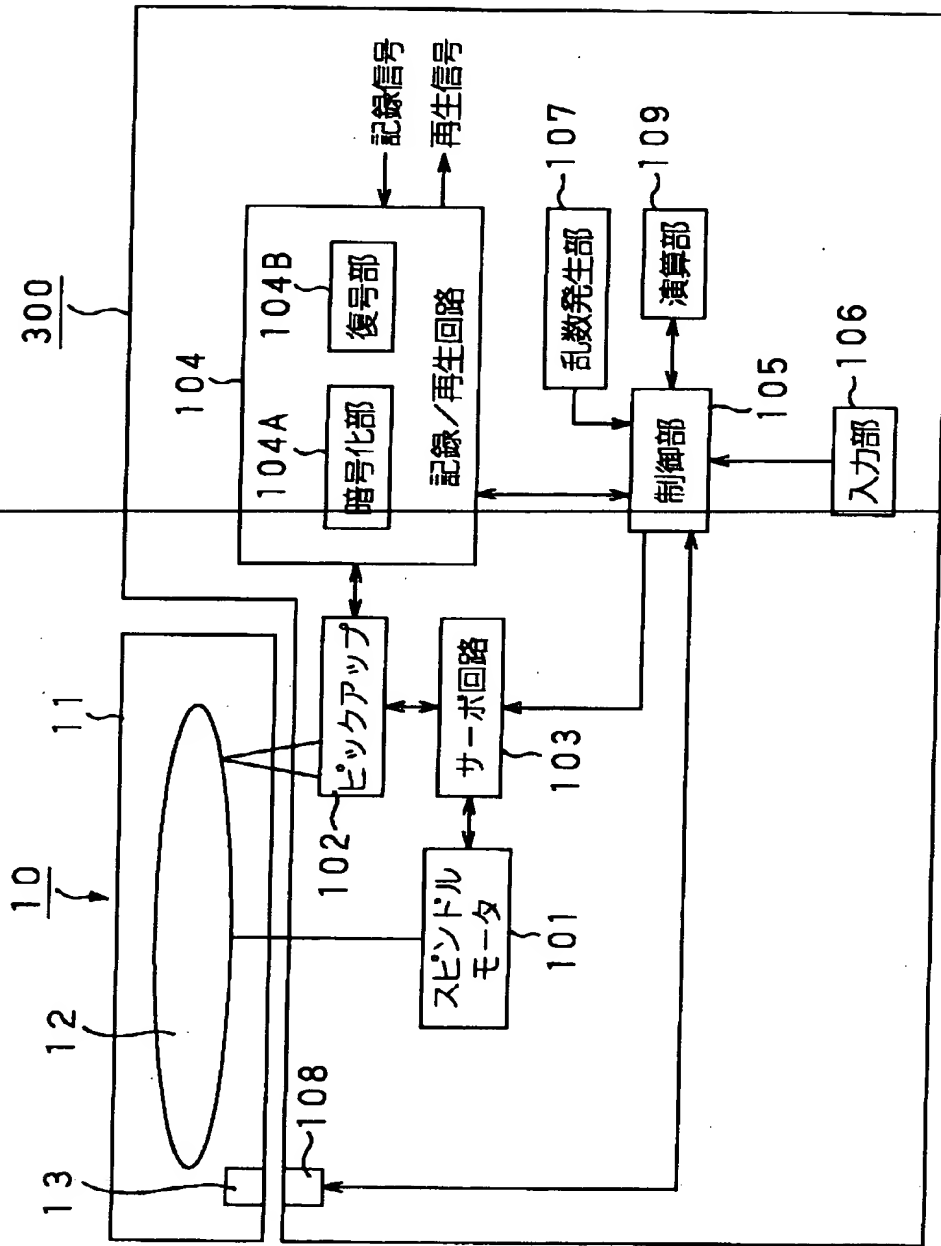
【図 6 3】



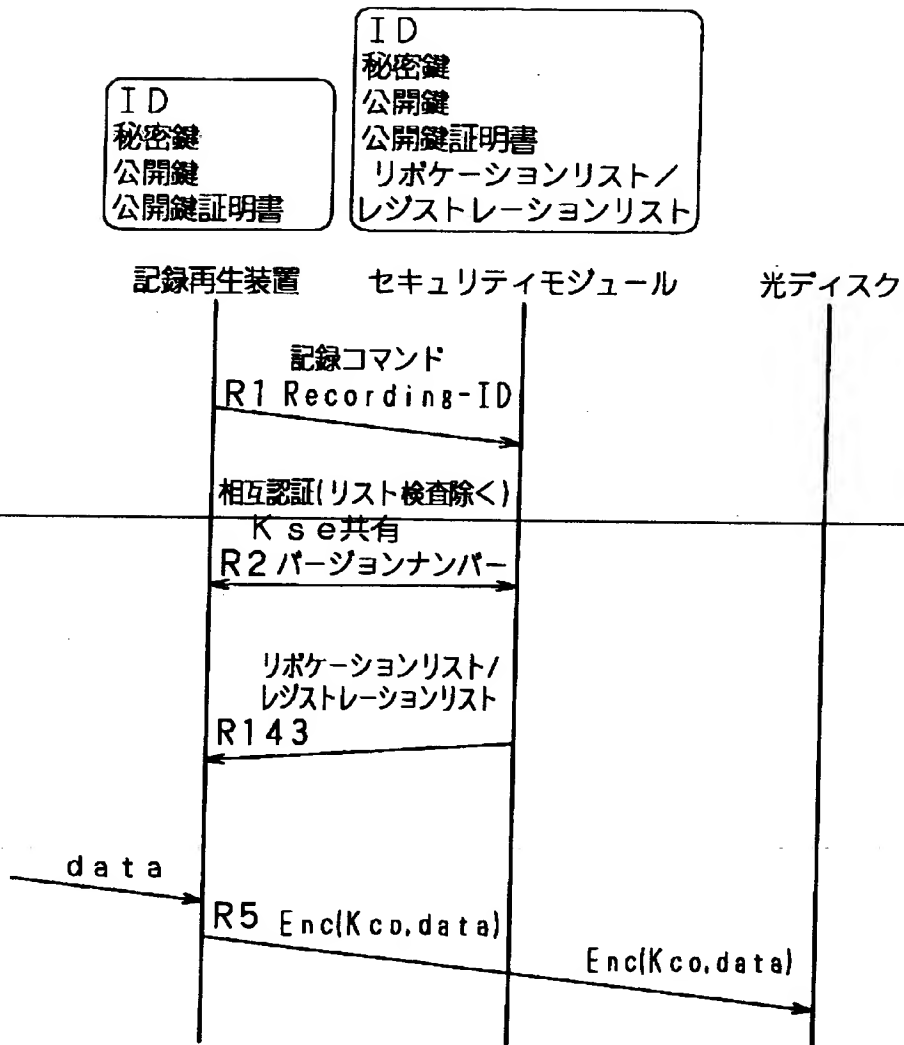
【図 6 4】



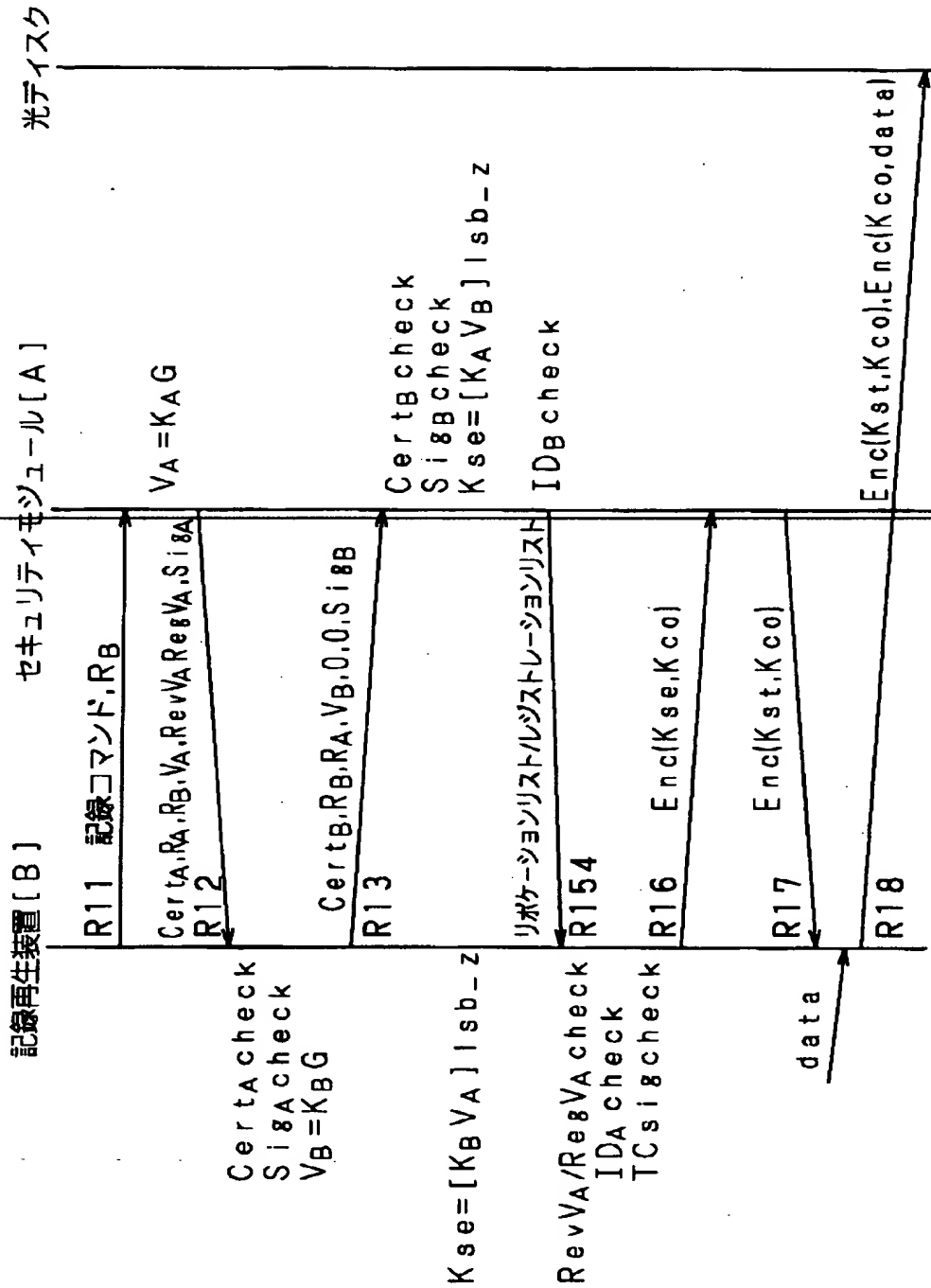
【図 6 5】



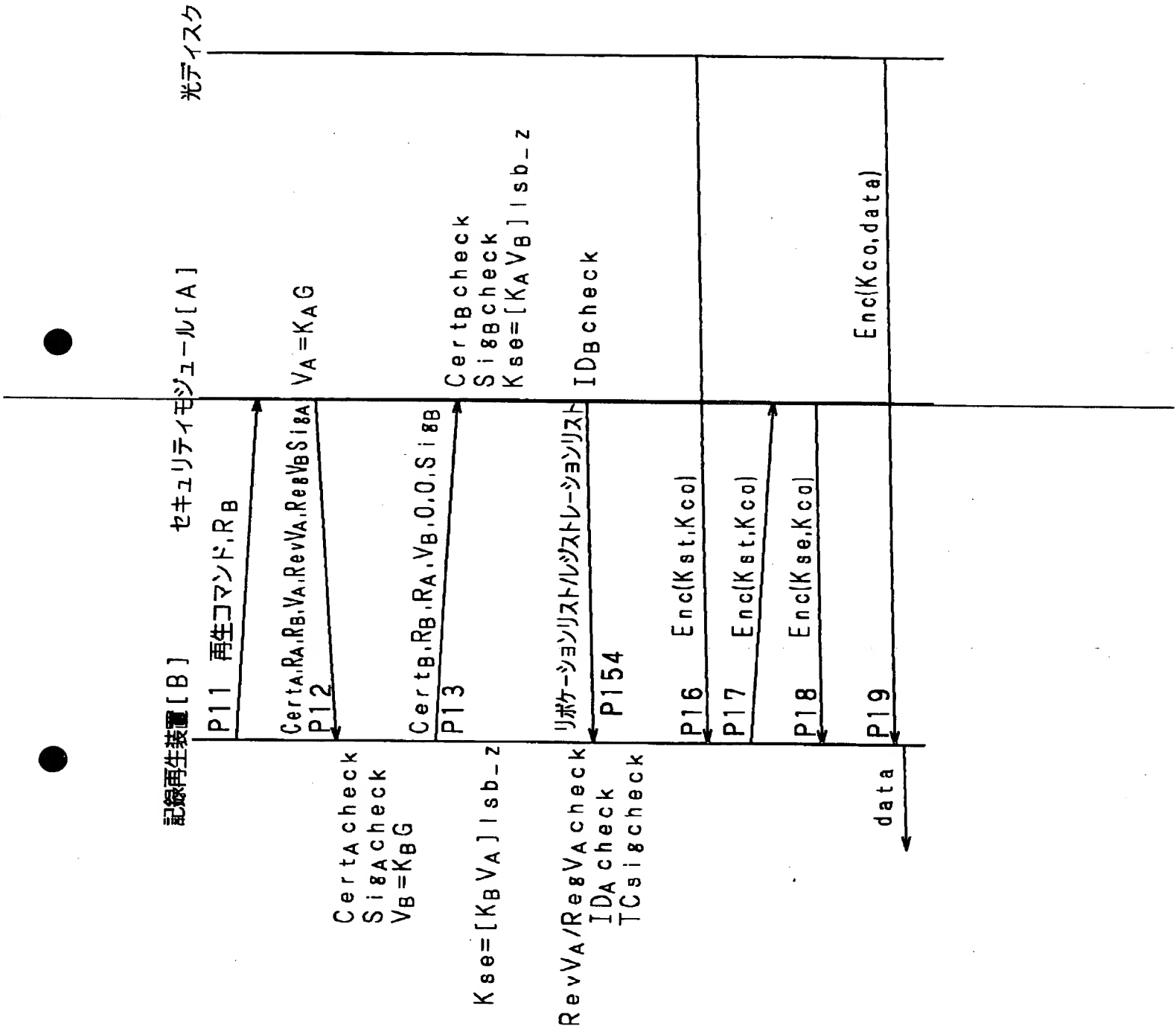
【図 6 6】



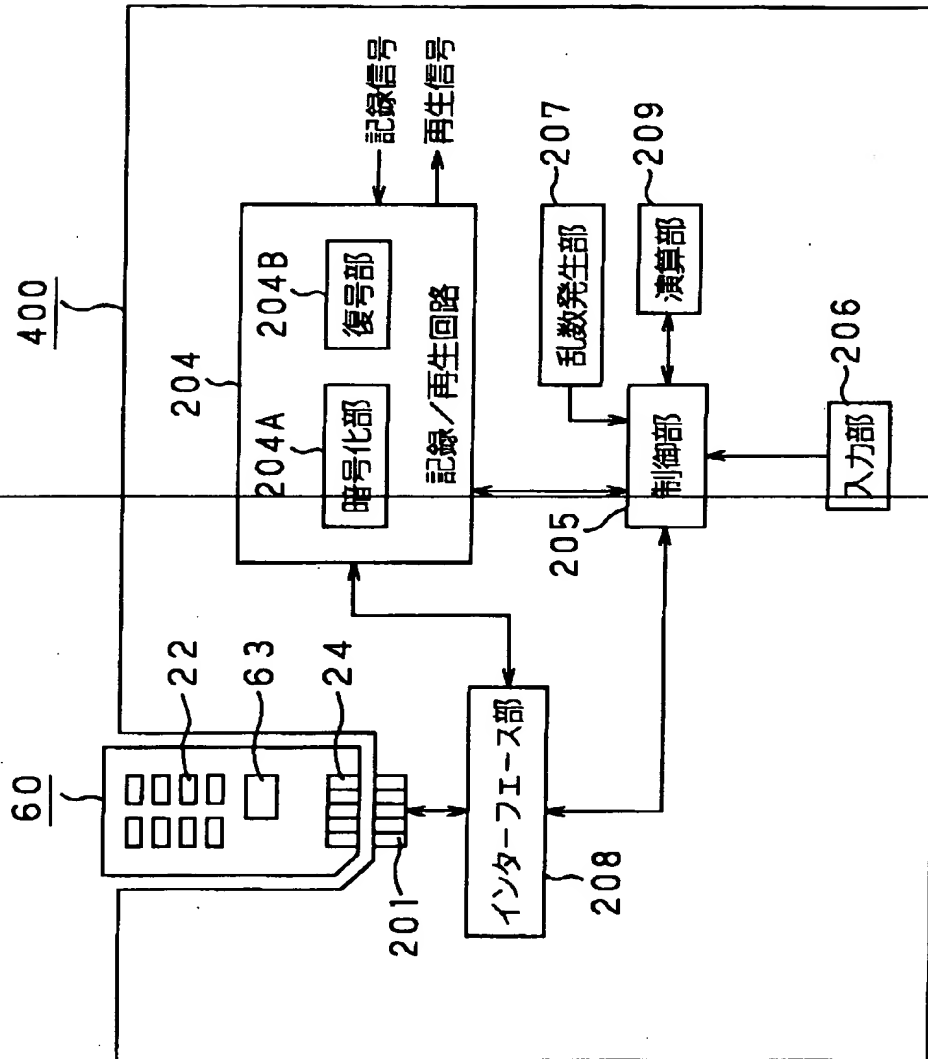
【図 6 7】



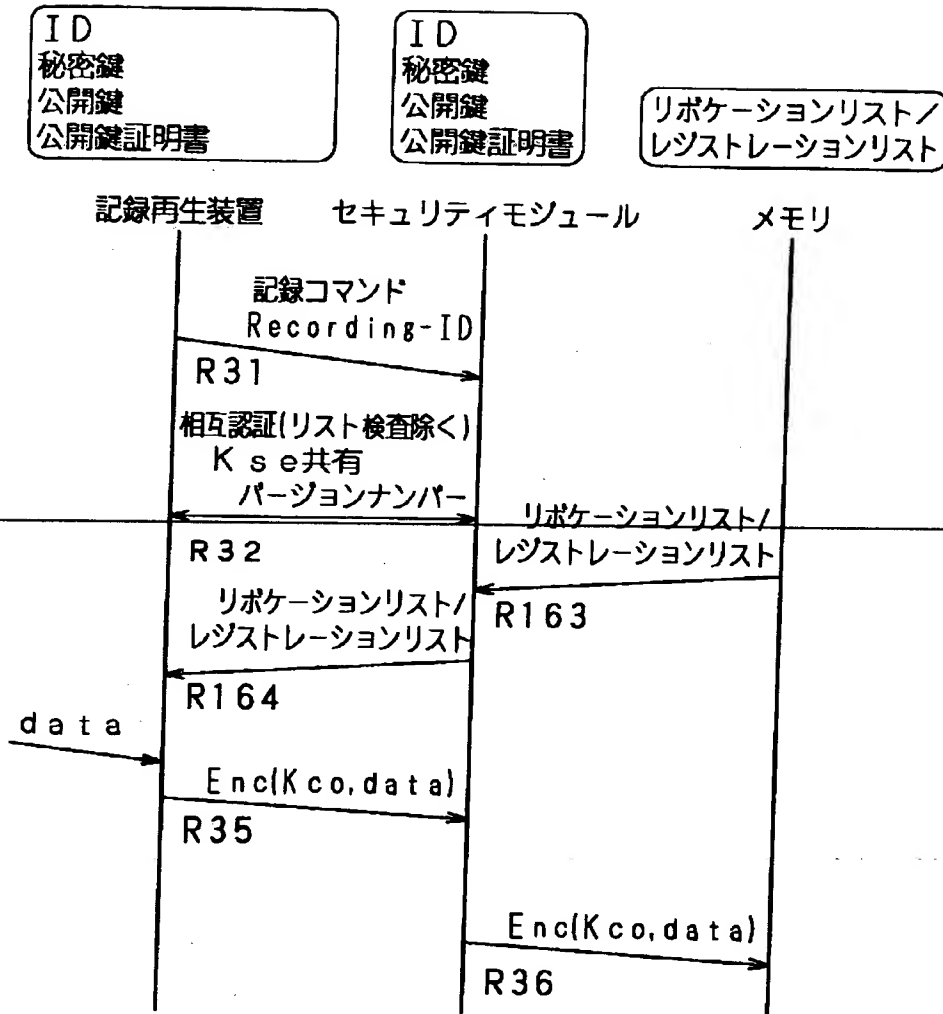
【図 6 8】



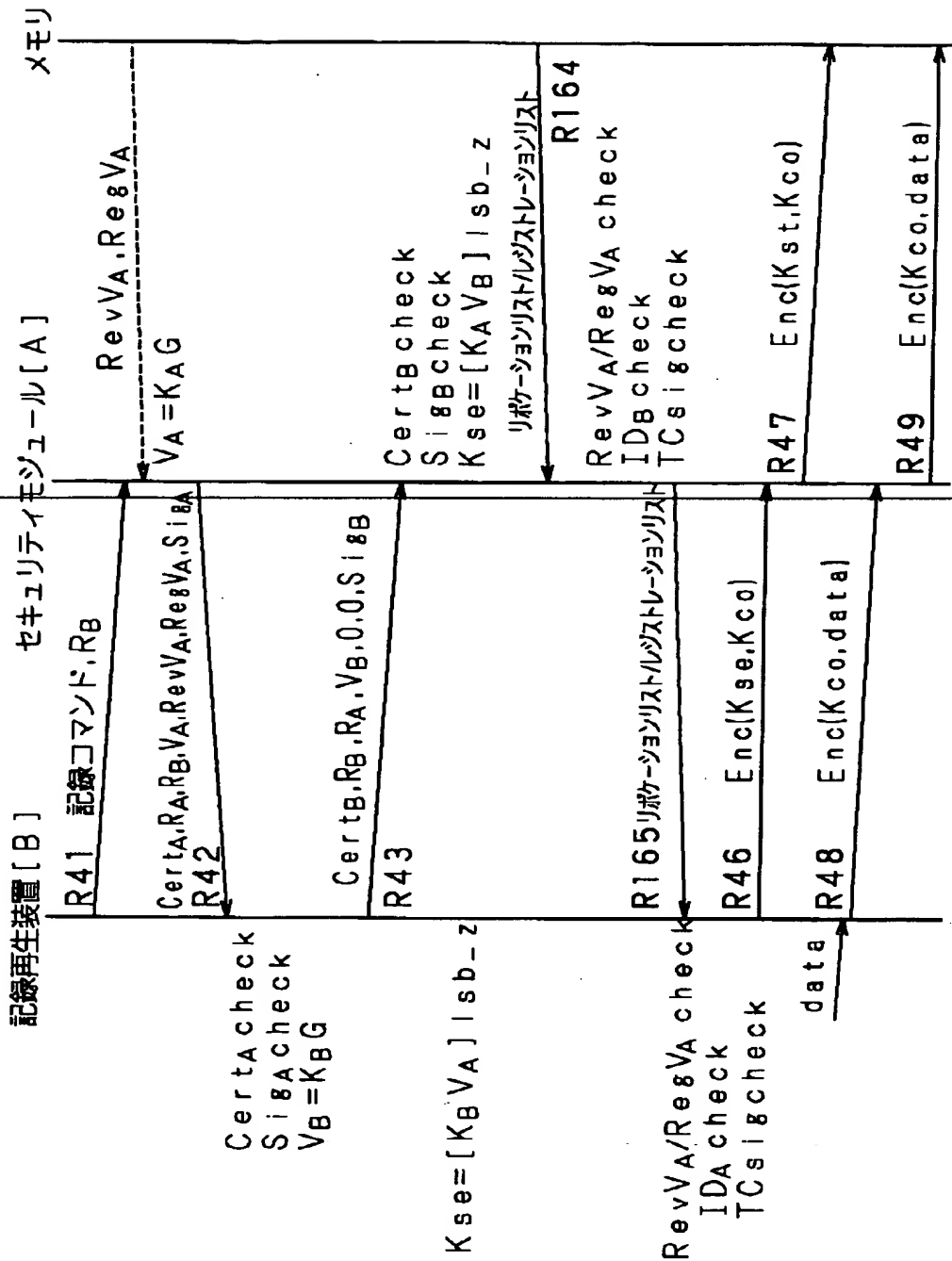
【図 6 9】



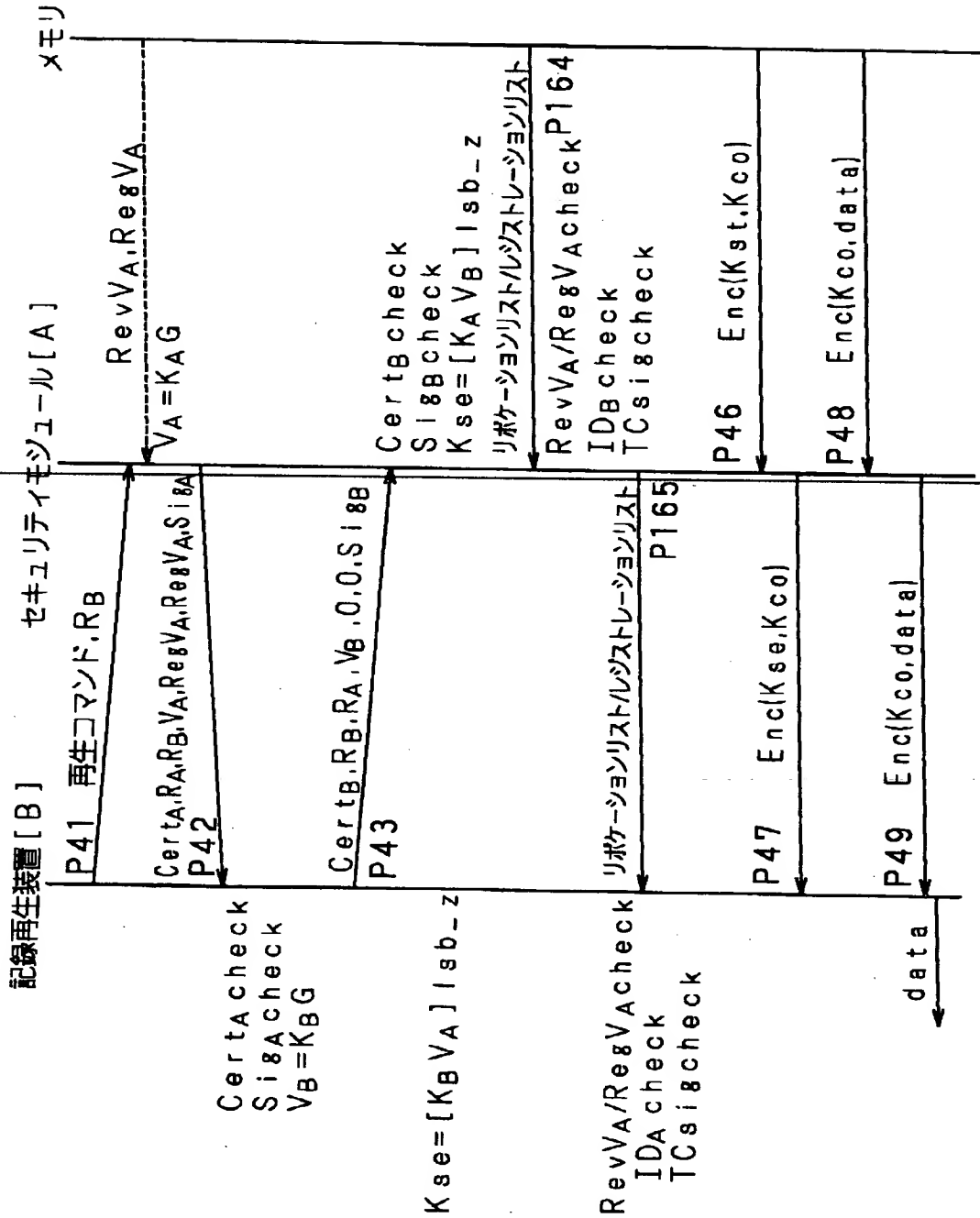
【図 70】



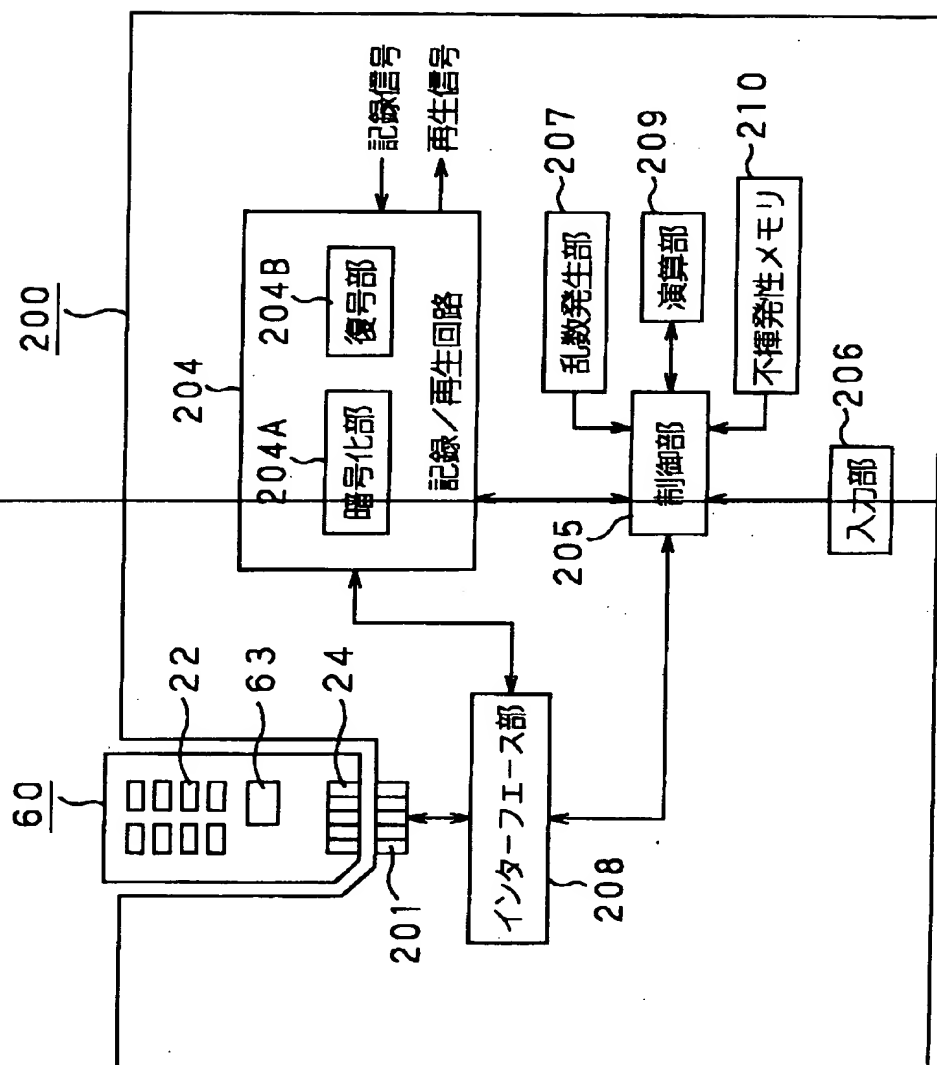
【図 7 1】



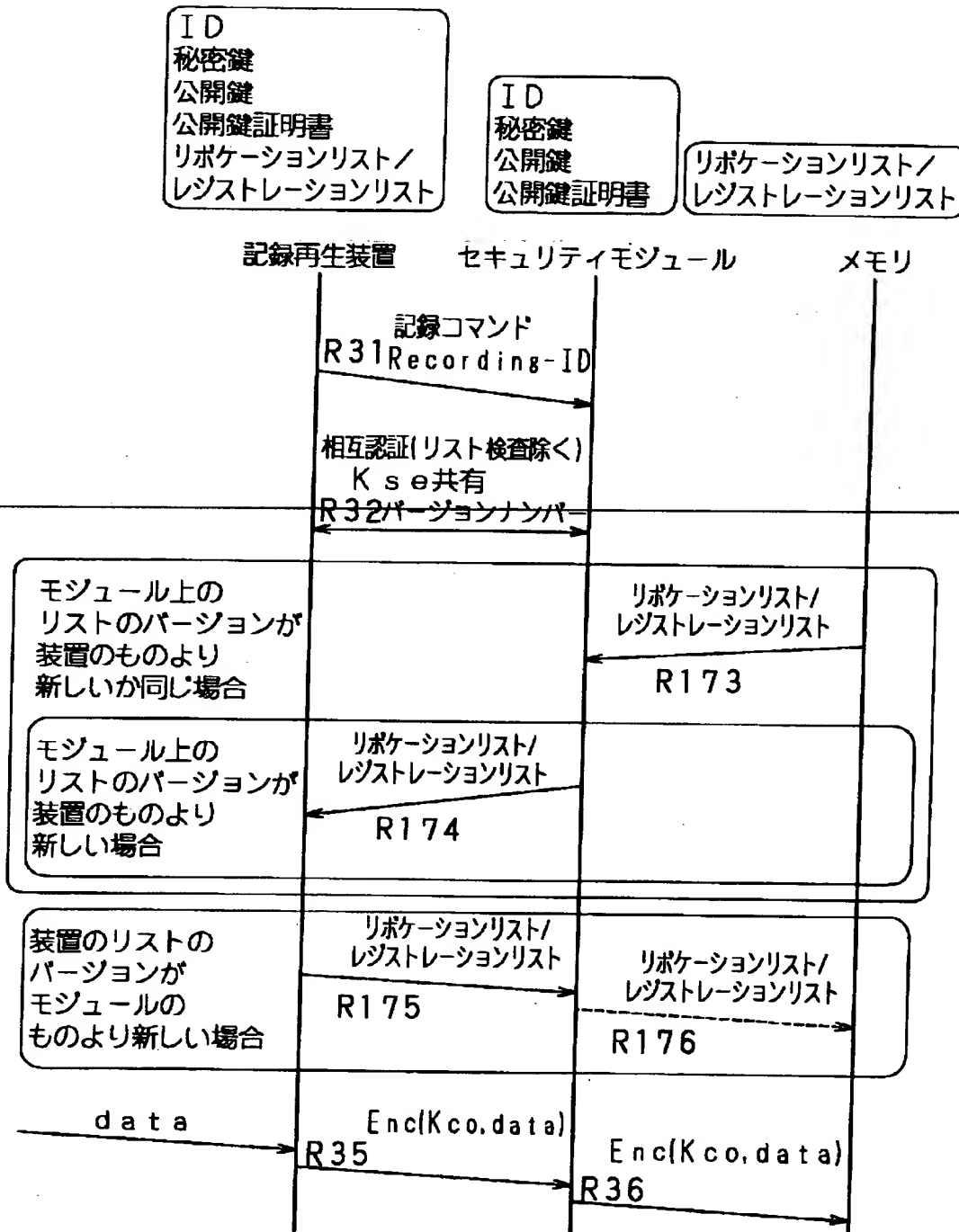
【図 7 2】



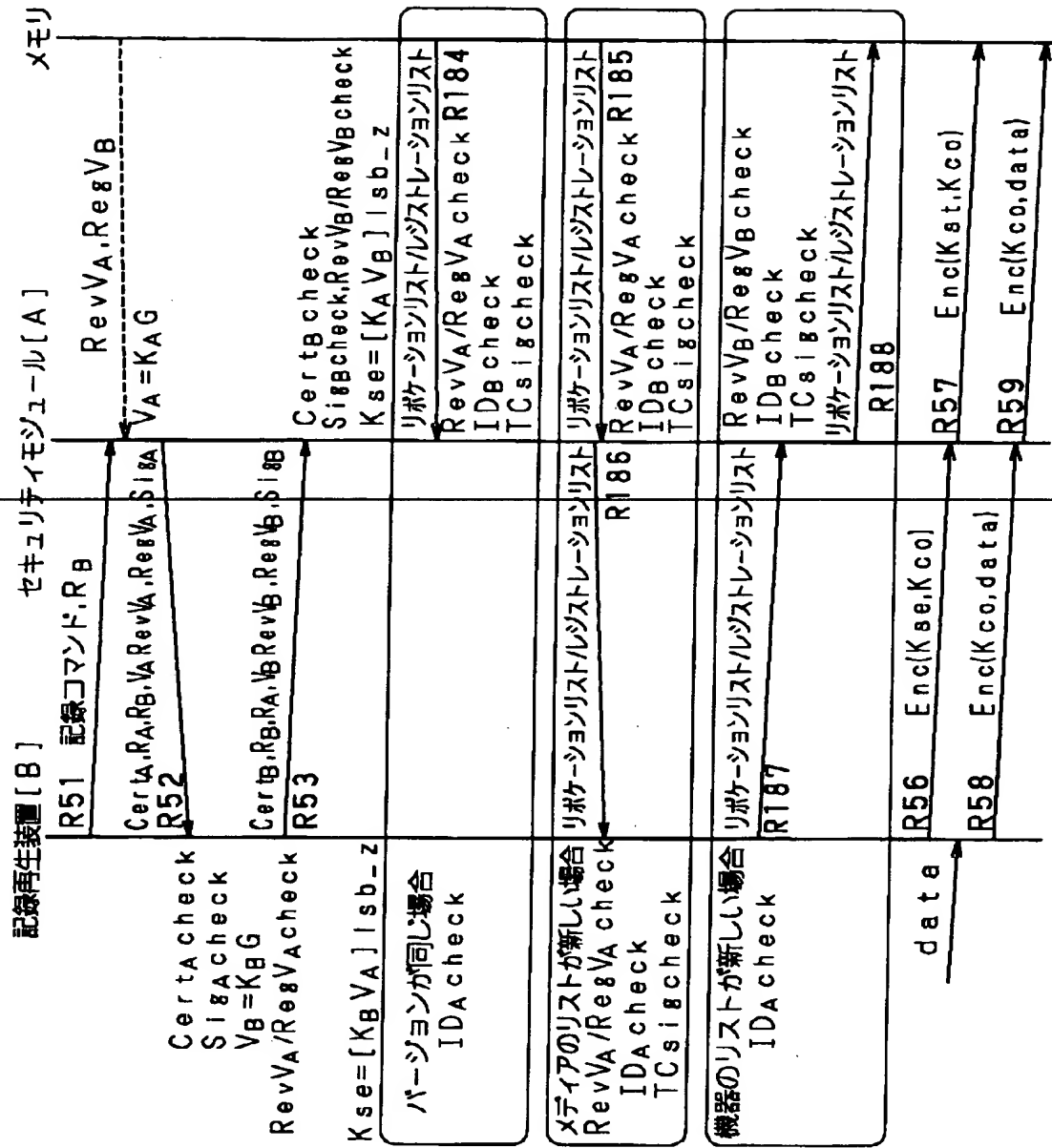
【图 7 3】



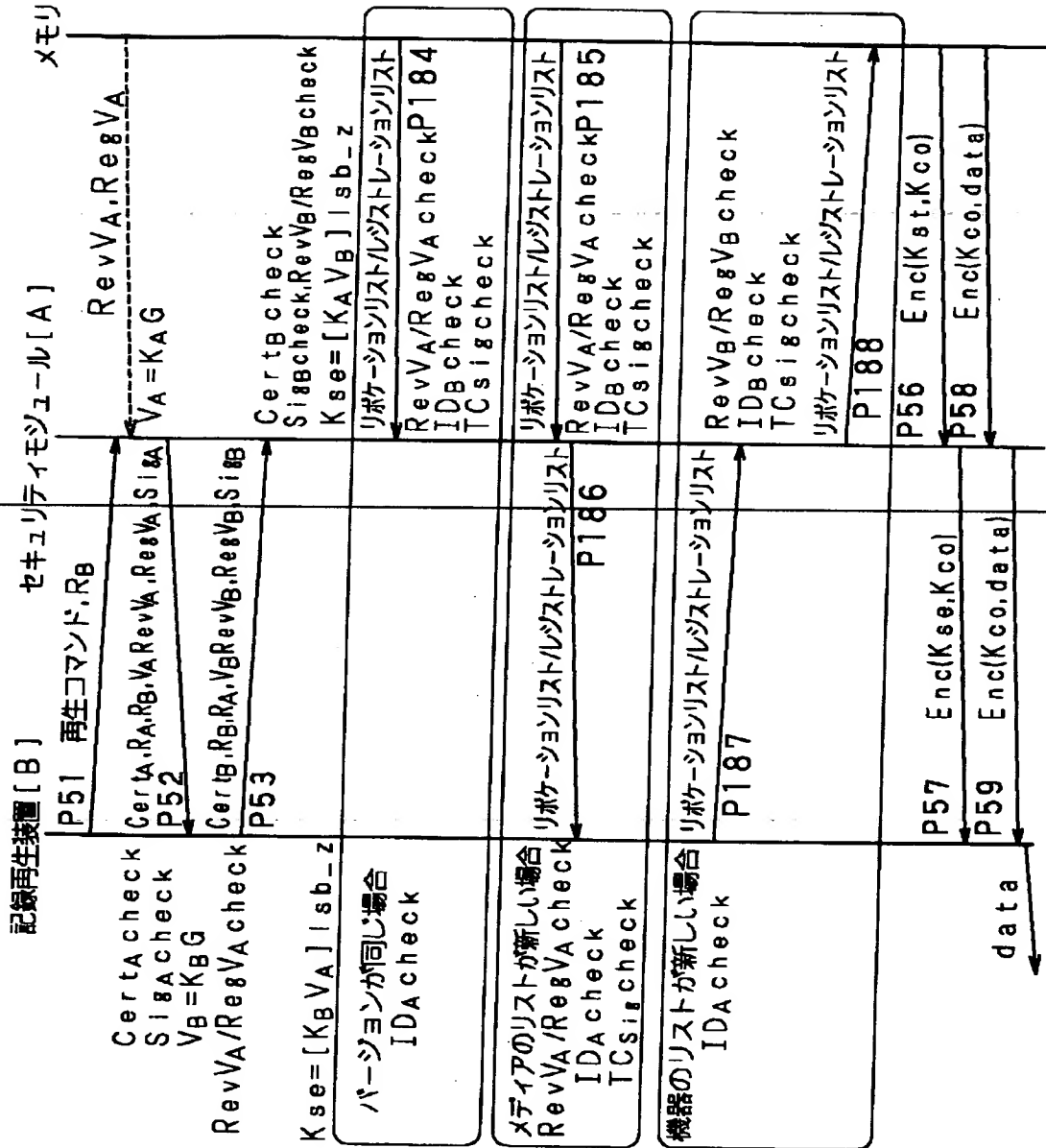
【図 7 4】



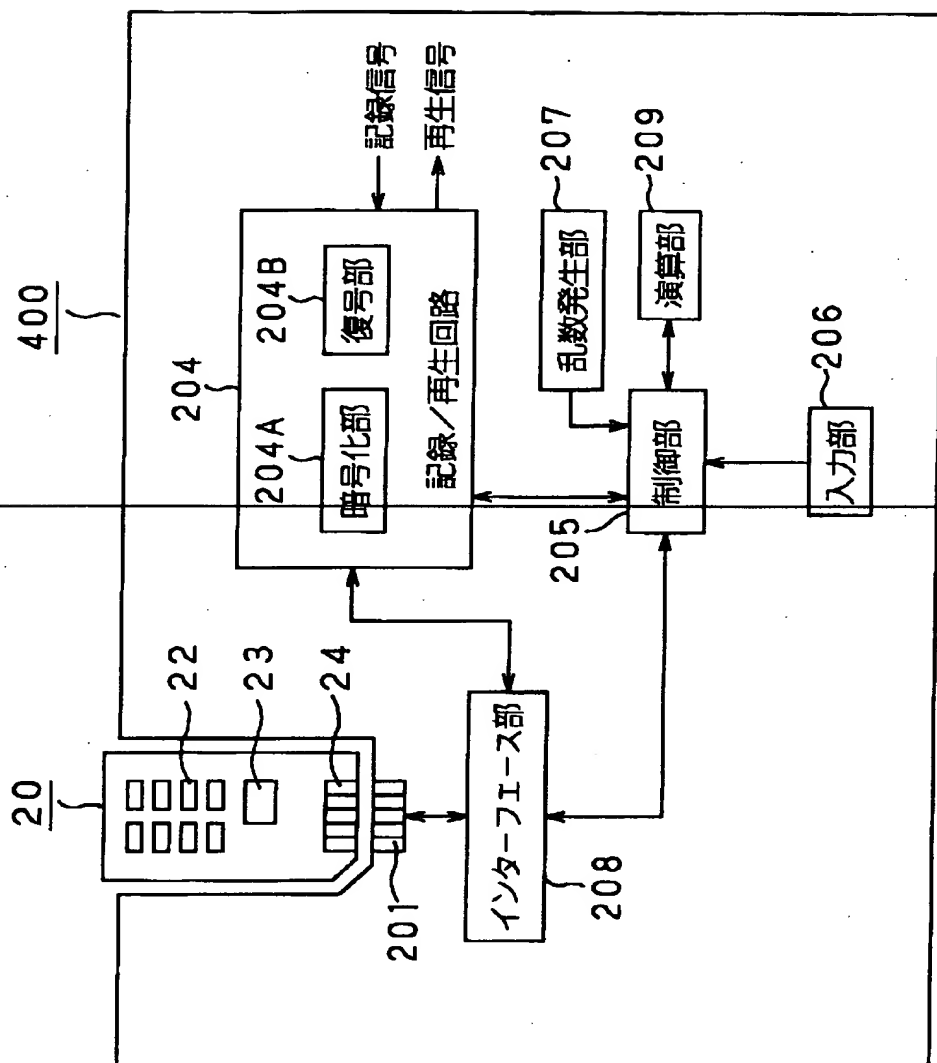
【図 7 5】



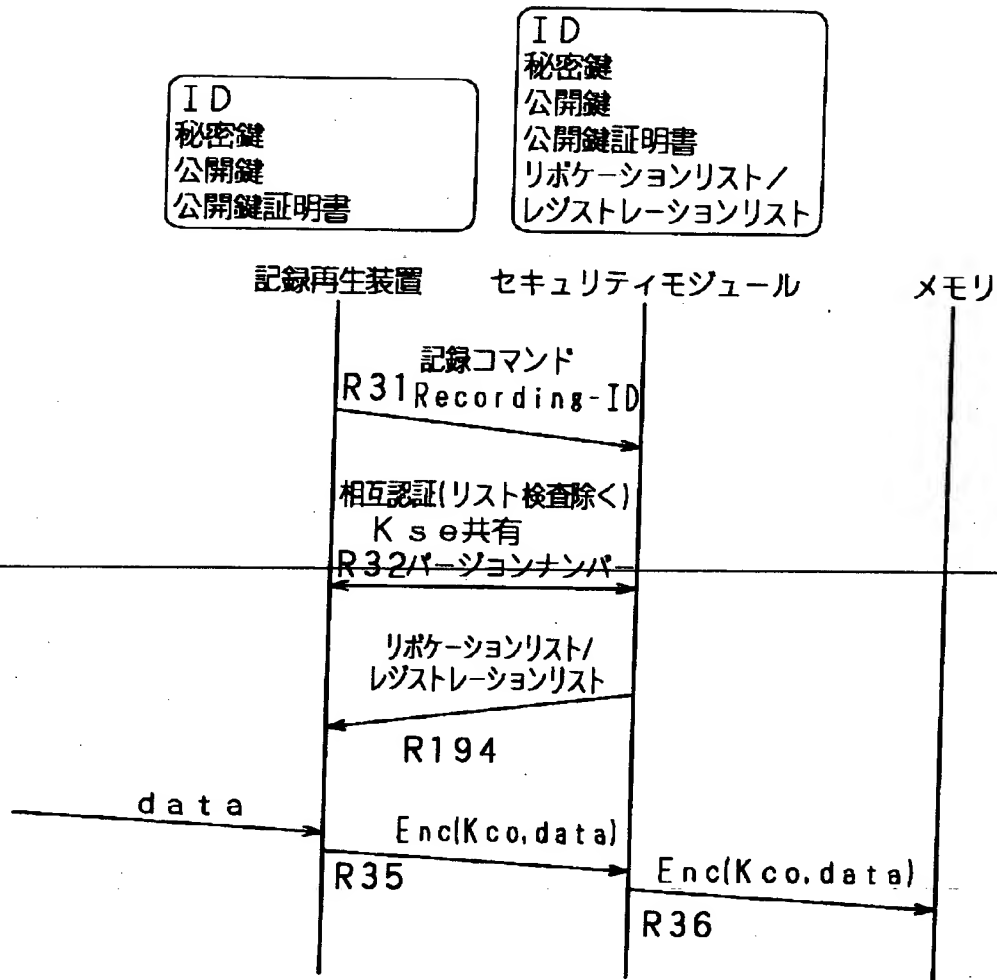
【図 7 6】



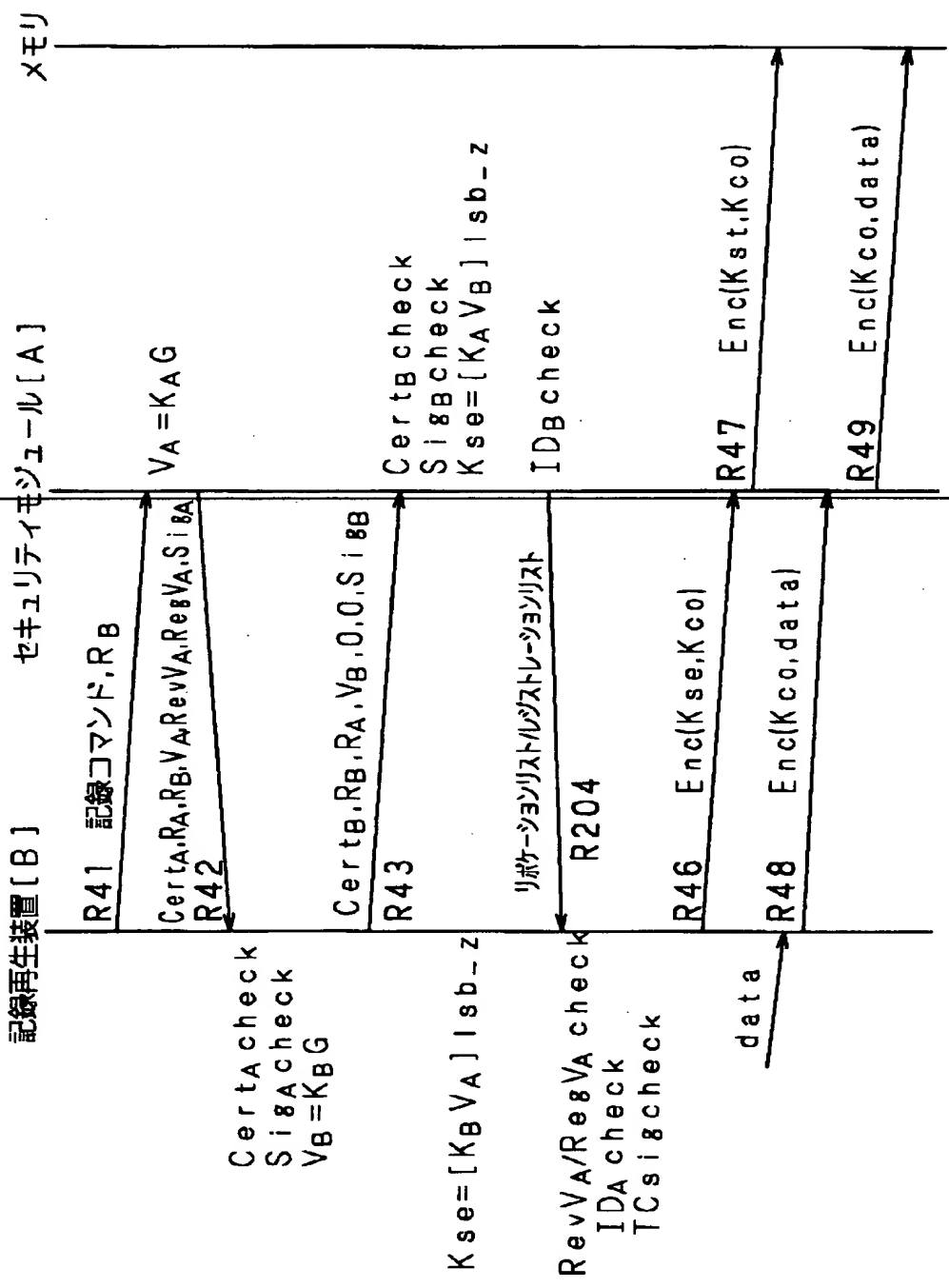
【図 7 7】



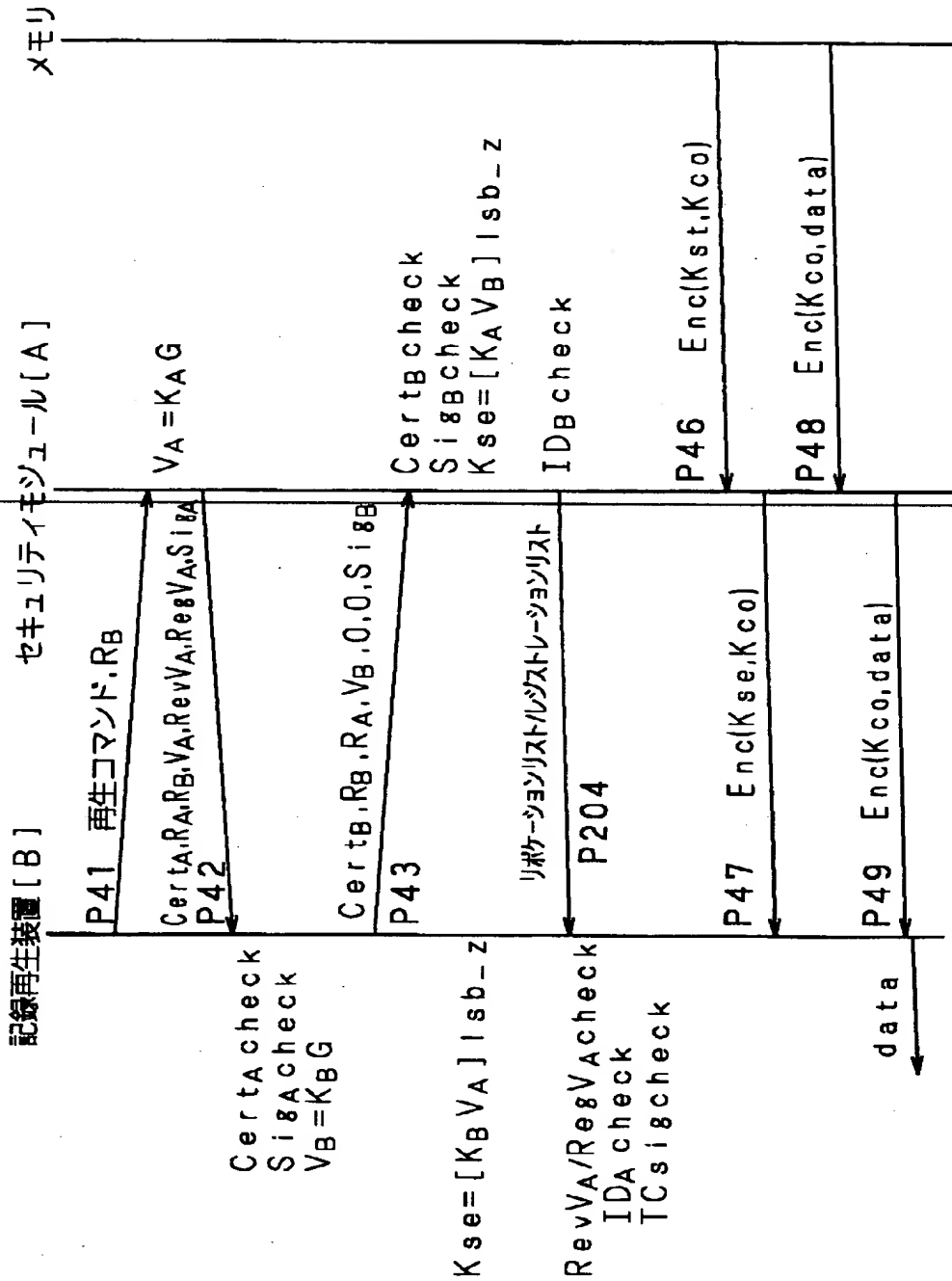
【図 7 8】



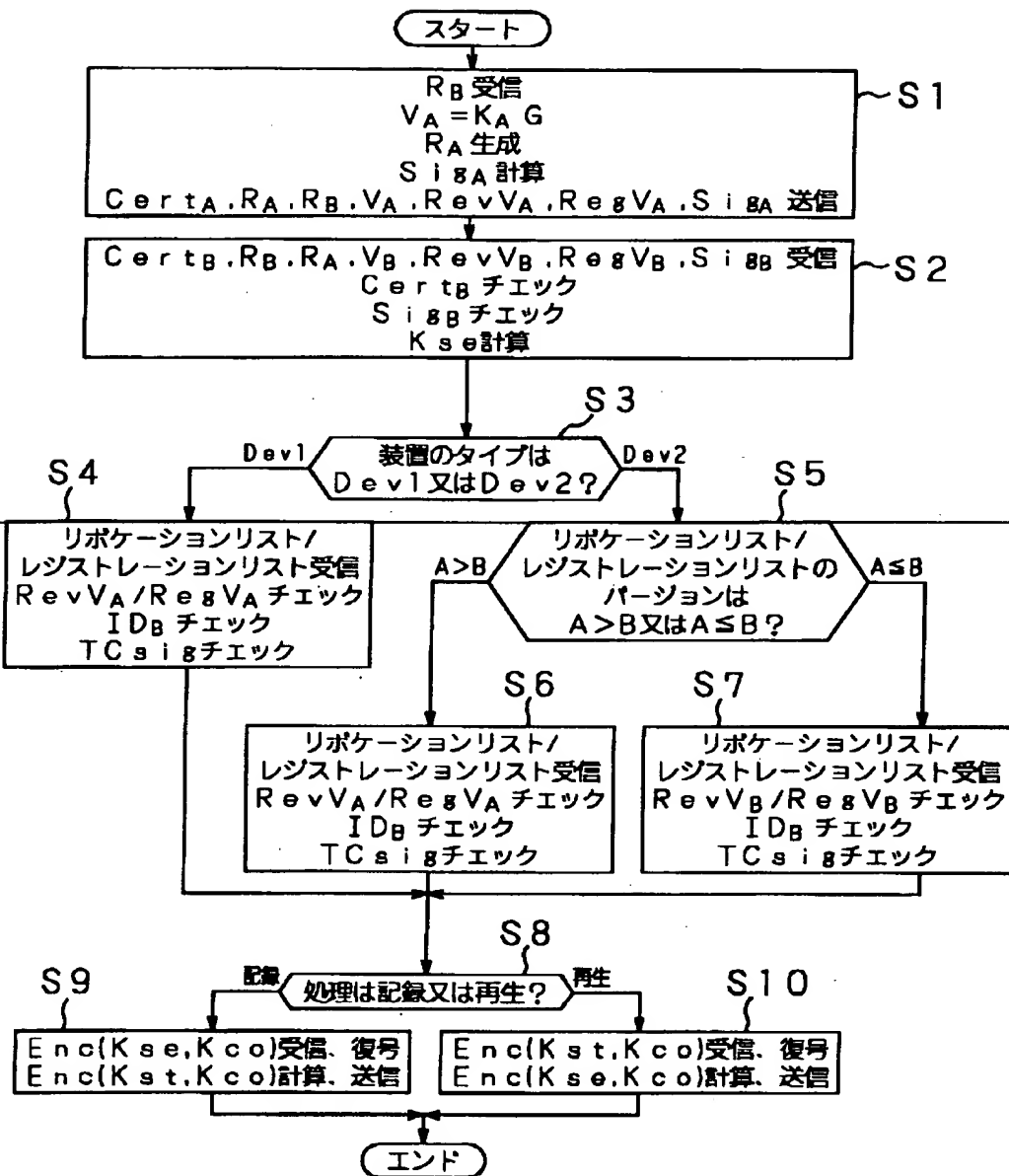
【図 7 9】



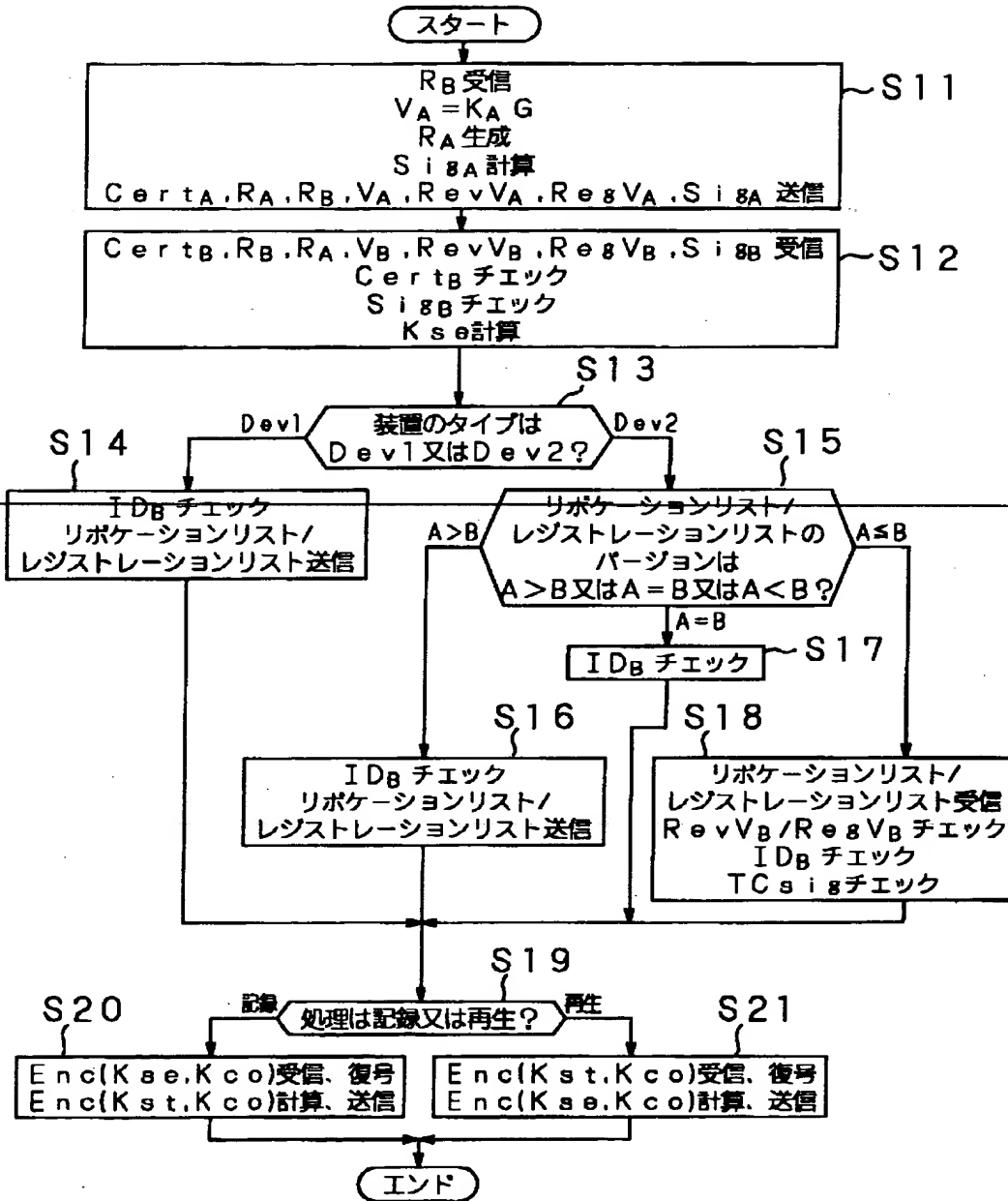
【図 8 0】



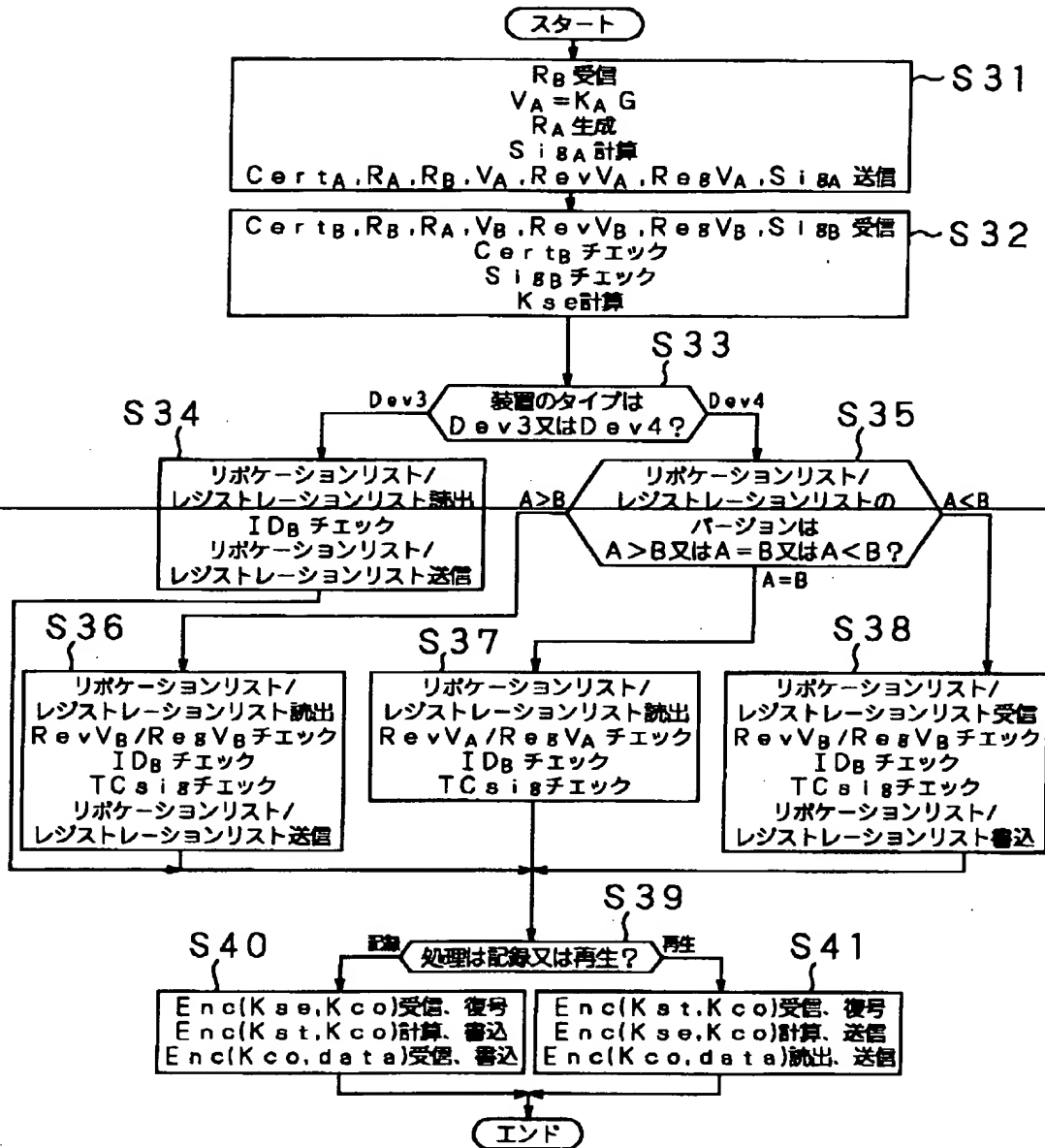
【図 81】



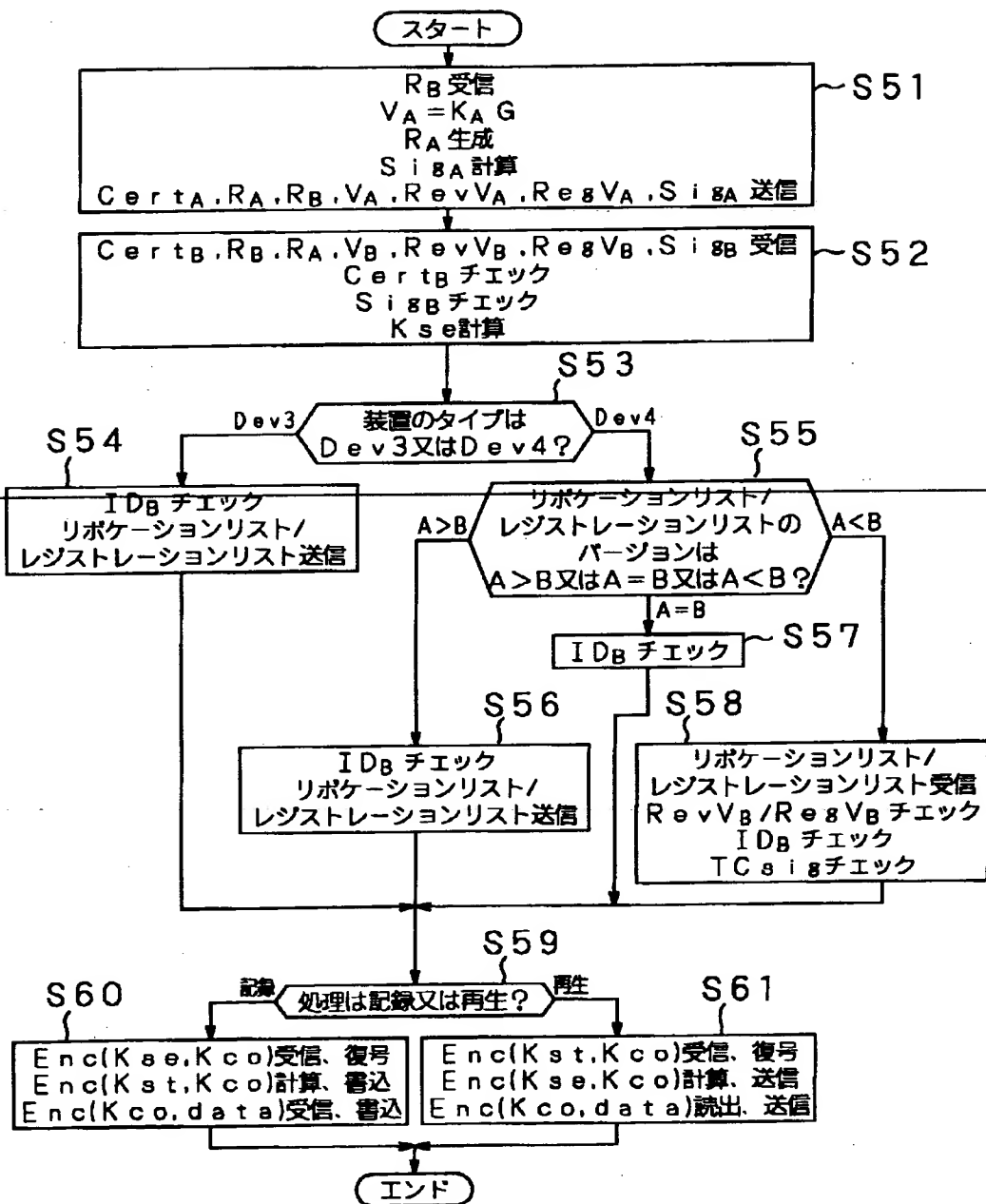
【図 82】



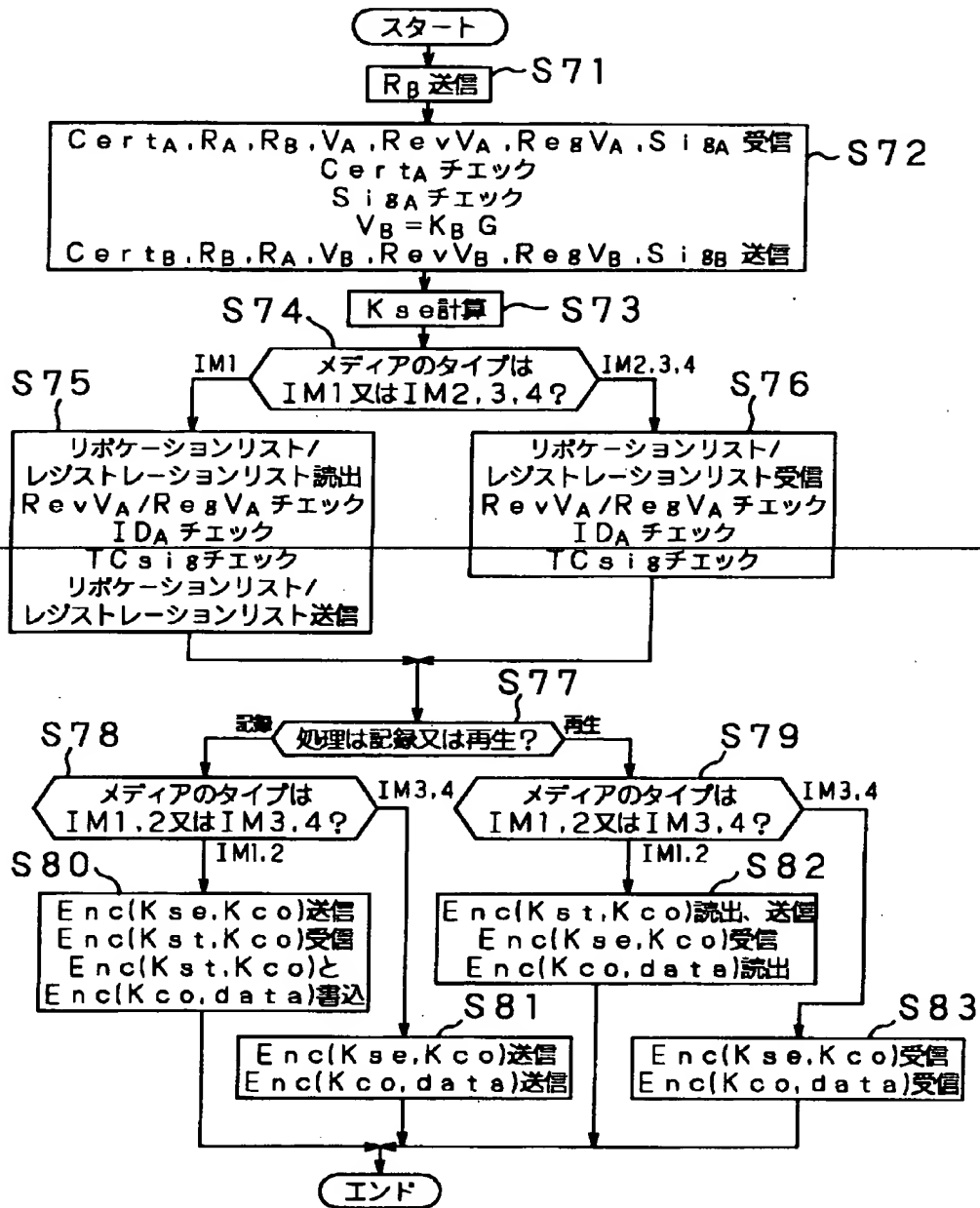
【図 8 3】



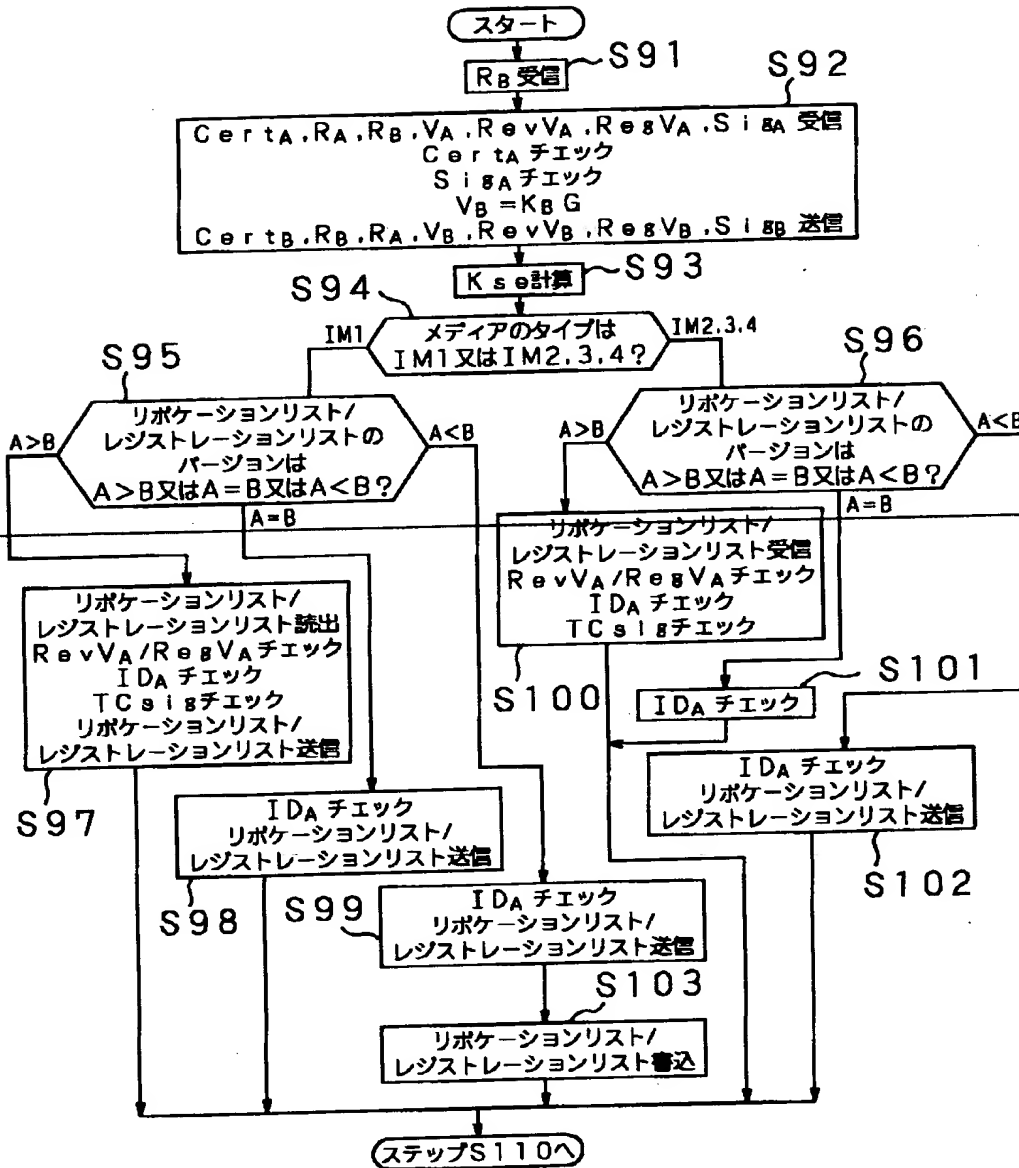
【図 8 4】



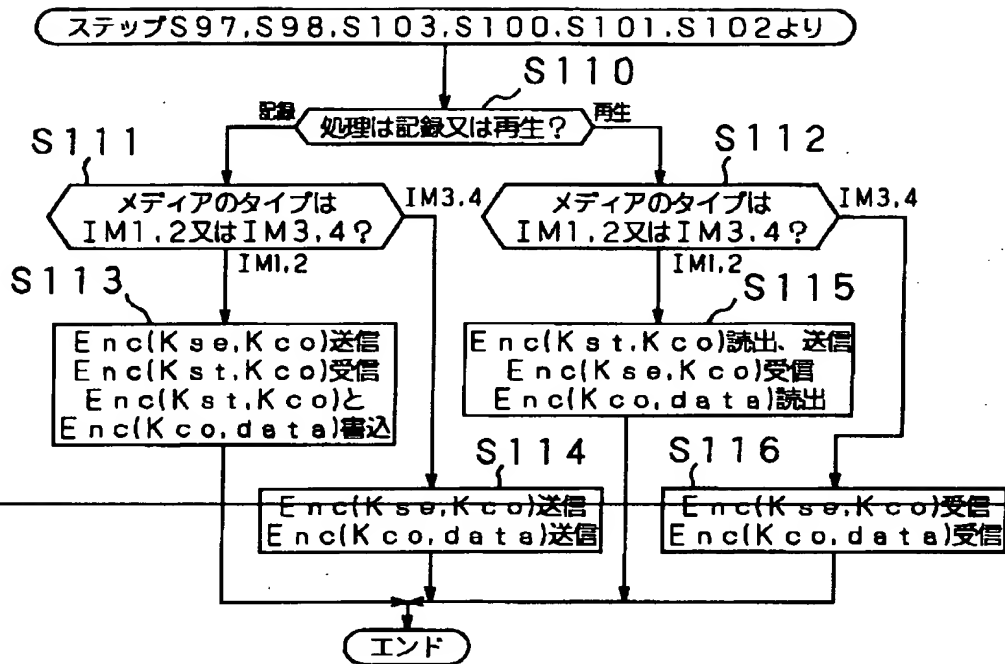
【図 85】



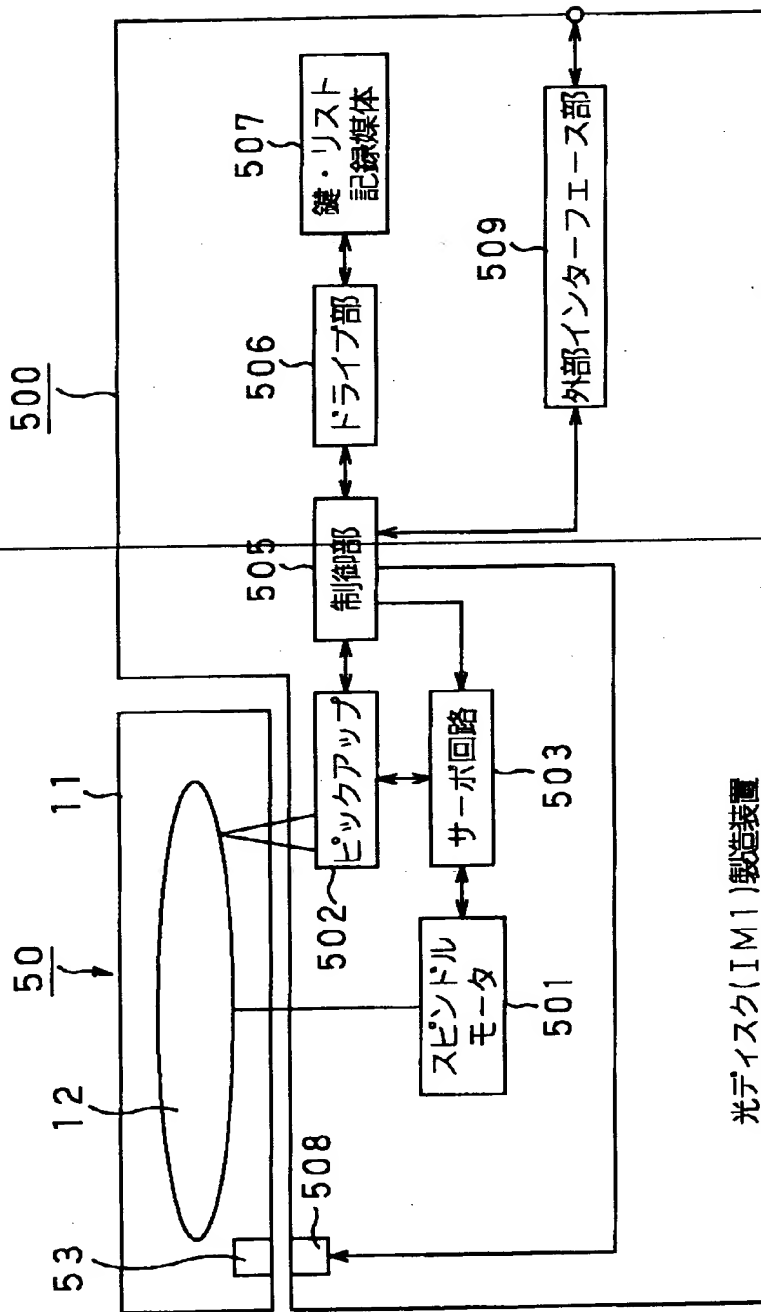
【図 86】



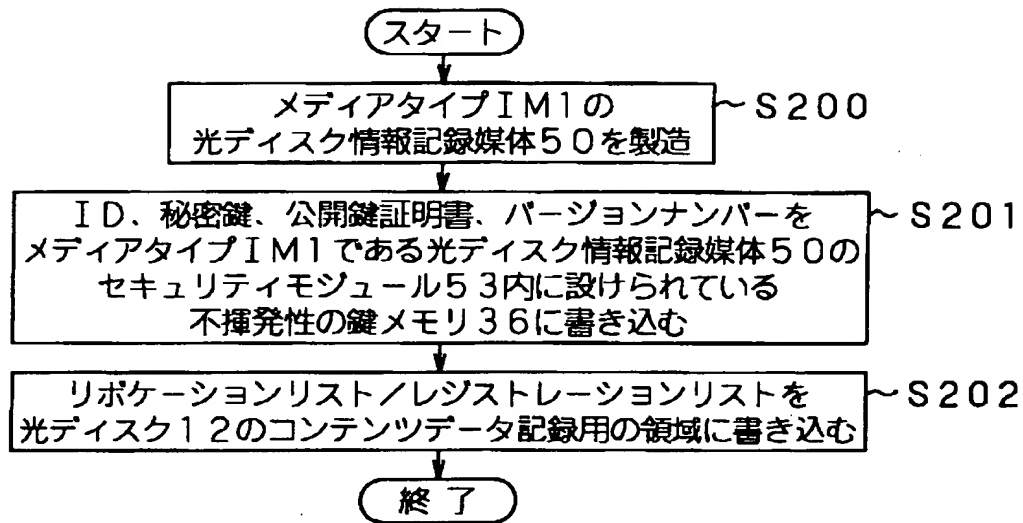
【図 87】



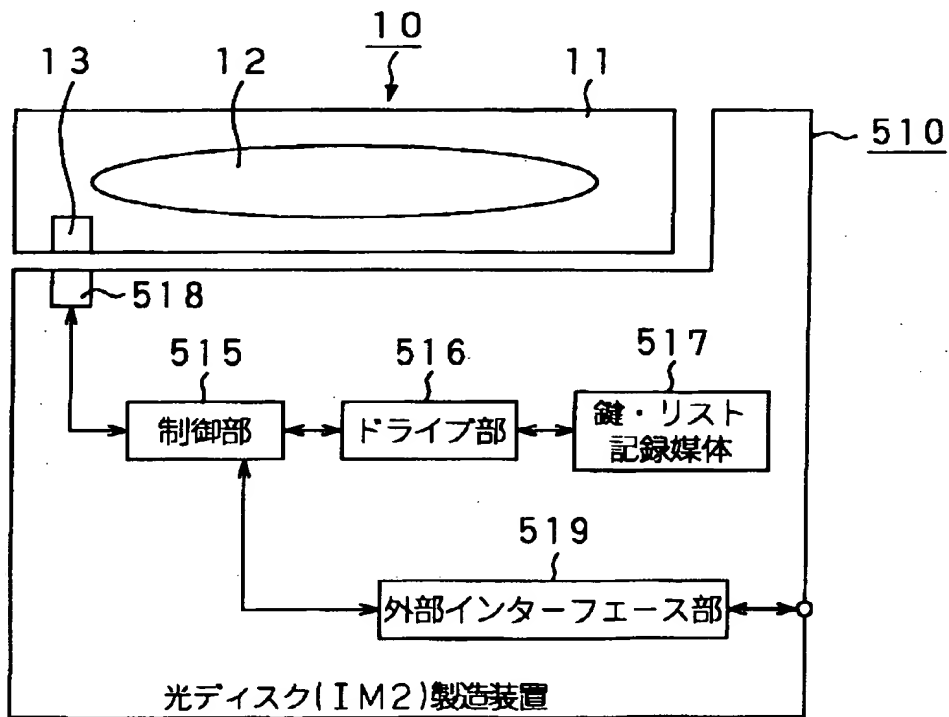
【図 8 8】



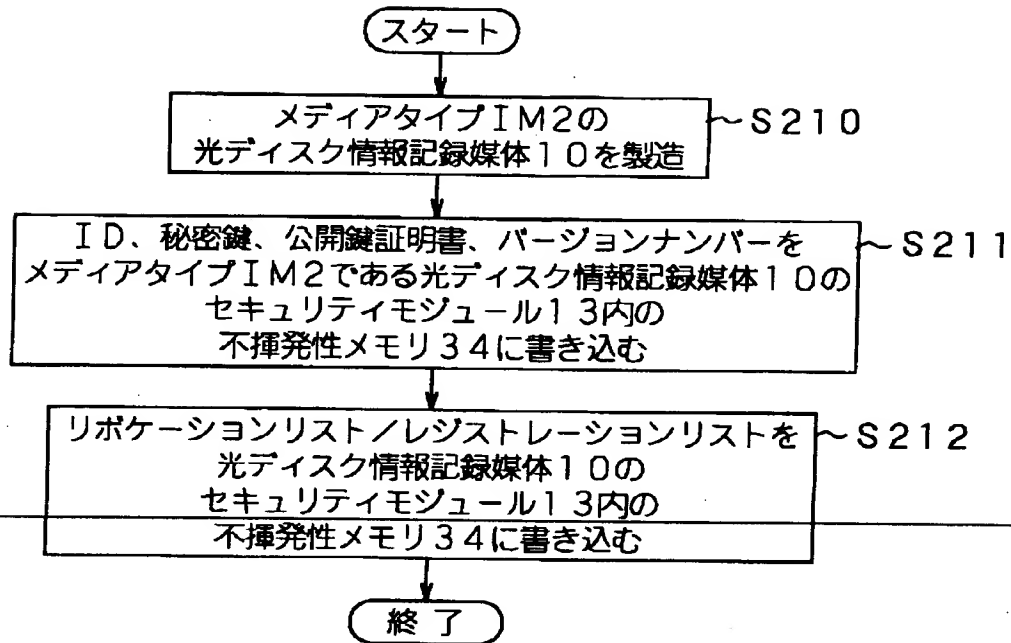
【図 89】



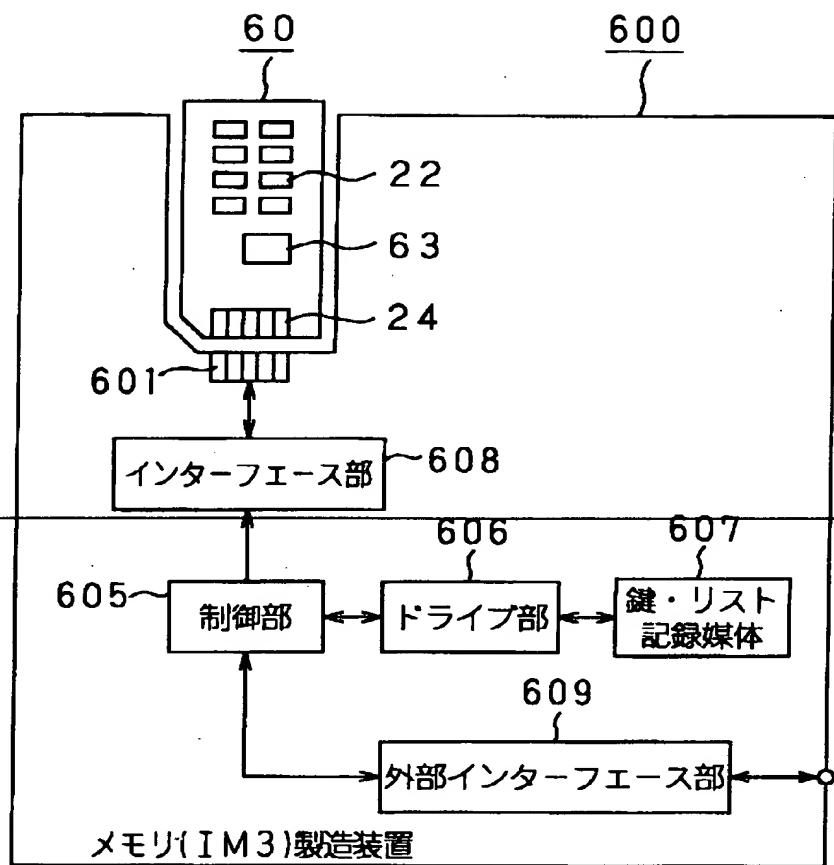
【図 90】



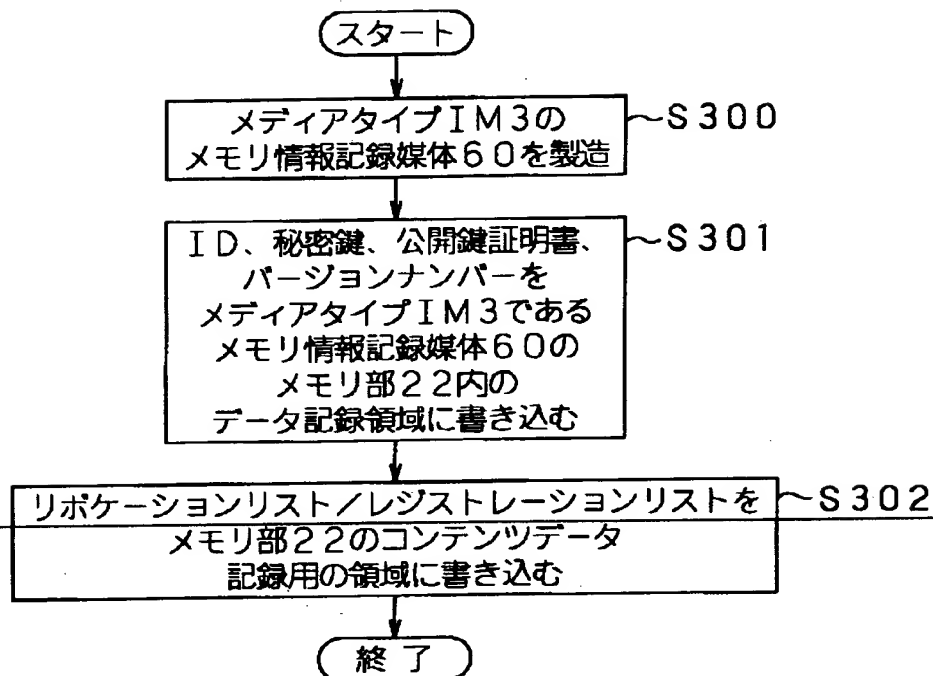
【図 9 1】



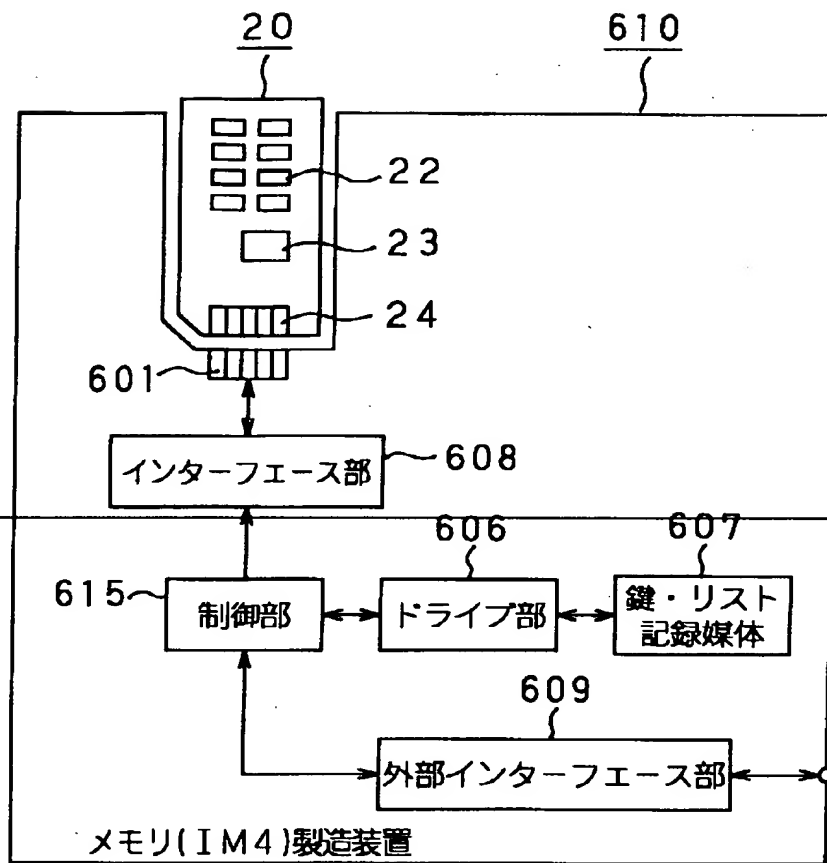
【図 9 2】



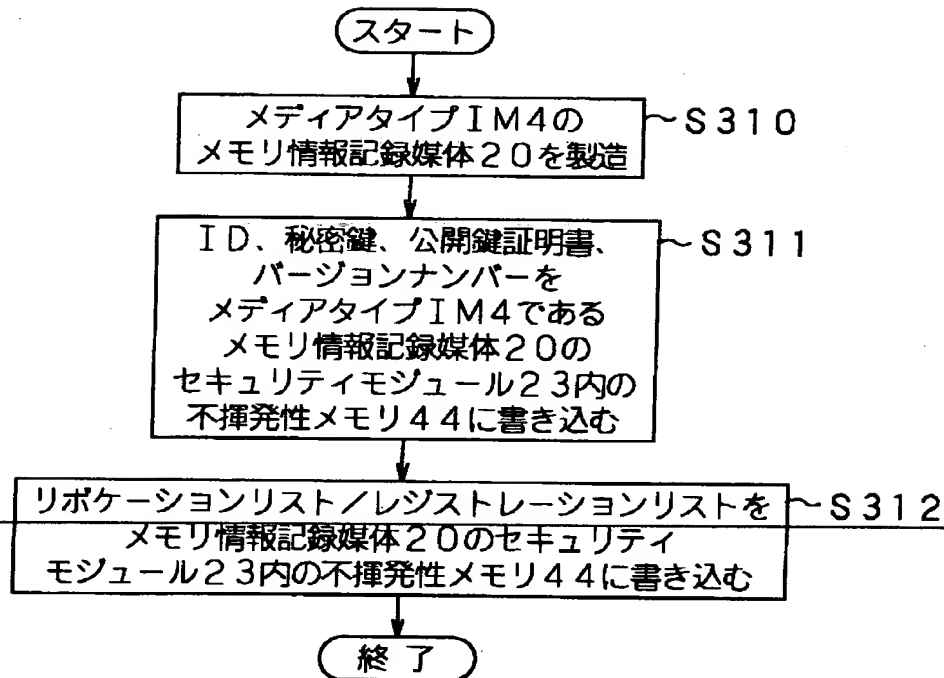
【図 9 3】



【図 9 4】



【図 9 5】



【書類名】 要約書

【要約】

【課題】 映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことができるようにする。

【解決手段】 光ディスク情報記録媒体 1 0 にセキュリティモジュール 1 3 を持たせ、光ディスク上に記録されるデータを個々のデータ毎に異なる暗号鍵で暗号化し、暗号鍵をセキュリティモジュール 1 3 が安全に保管する。また、セキュリティモジュール 1 3 は、記録再生装置と公開鍵暗号技術を用いた相互認証を行い、相手が正当なライセンスを受けた装置であることを確認した上で、暗号鍵を装置に対して与えることにより、不正な装置にはデータを漏らさないようにする。

【選択図】 図 1

認定・付加情報

特許出願の番号	平成 11 年 特許願 第 3 6 3 2 6 6 号
受付番号	5 9 9 0 1 2 4 7 9 6 4
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 12 年 1 月 6 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川 6 丁目 7 番 3 5 号
【氏名又は名称】	ソニー株式会社
【代理人】	申請人

【識別番号】	100067736
【住所又は居所】	東京都港区虎ノ門 2-6-4 第 11 森ビル 小池国際特許事務所
【氏名又は名称】	小池 晃

【選任した代理人】

【識別番号】	100086335
【住所又は居所】	東京都港区虎ノ門 2 丁目 6 番 4 号 第 11 森ビル 小池国際特許事務所
【氏名又は名称】	田村 榮一

【選任した代理人】

【識別番号】	100096677
【住所又は居所】	東京都港区虎ノ門二丁目 6 番 4 号 第 11 森ビル 小池国際特許事務所
【氏名又は名称】	伊賀 誠司

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社

THIS PAGE BLANK (USPTO)